NATIONAL SECURITY AUTHORITY

REPORT ON CYBER SECURITY

of Slovak Republic in 2022

NATIONAL SECURITY AUTHORITY

REPORT ON CYBER SECURITY

of Slovak Republic in 2022

CONTENTS

1 INTRODUCTION

The year 2022 has shown us that cyber warfare has become an essential part of our society. Cyber-attacks are not the invention of technology enthusiasts. They are actively used in military conflicts, such as Russia‘s war against Ukraine, in intelligence games and in criminal activities.

The report on cyber security in the Slovak Republic in 2022 illustrates the current situation in this area from a global and national perspective. It focuses on the most significant events and threats and, on the basis of the collected data, attempts to assess the activities and performance of relevant actors.

The data comes from the activities of the National Cyber Security Centre SK-CERT, the Cyber Security Competence and Certification Centre (CSCCC) and other relevant entities, especially when looking at the issue from a sectoral perspective. They also cover global trends in 2022 and take a look at threats and incidents in Slovak cyberspace, as well as information on education and activities in this area.

Last year was marked in particular by the beginning of Russia‘s war against Ukraine. The cyber-attacks associated with this war were not isolated to the territory of occupied Ukraine, but affected a number of states, particularly those that were actively supporting Ukraine either militarily or on a humanitarian basis. The year 2022 has shown us that well-prepared risk assessment and risk management, consistent implementation of security measures and mutual cooperation are the path to success.

2 THREATS AND INCIDENTS OVERVIEW OF 2022

Global cyberspace in 2022 was most significantly impacted by Russia‘s war against Ukraine. In addition to the use of conventional weapons in the physical world, it meant launch of cyber operations – even before the outbreak of war.

2.1 Russia’s war against Ukraine

Prior to the conflict, the Russian side was conducting cybertical offensive operations that were to cause dis-improving the functioning of the services and functions of state organizations and critical infra-structure. After the outbreak of conflict, most of the existing hacker group sin the region has joined one of the parties involve. The rest, however, retained their standard operating models.

During the war, new community hacker movements have been established. One of the first was the initiative of the group KILLNET, which founded the LEGION community movement. These are unique groupings that exchange informations, know-how, sharing of scripts, programs and program licenses between each other.

By then unknown people have gradually transformed into organized groups with hierarchical management and specialisation. They were coordinated through social networks, in particular on the Telegram communication platform, which also contributed to the involvement of a sympathetic public community into attacks.

Community movements have focused on hacking attacks for various purposes not only in Ukraine, but also in the region-nations that have actively and publicly supported Ukraine humanitarian or military. These targets were mainly member EU and NATO countries, including the Slovak Republic.

The most frequent activity of hacker groups and community movements were DDoS attacks that aimed to make websites and online services inaccessible. The choice of DDoS attack targets was tied to events in the real world as a donation of military material or open criticism of Russia. Choice of DDoS attack targets-was not always the most sophisticated. The attackers were mainly focused on the websites of state organizations (in some cases also private companies), whose unavailability had rather reputational consequences than practical implications for the functioning of the state and citizens. Over time, however, it was possible to see Increase in sophistication of target selection, tactics, techniques and tools used by the attacker. In some cases. DDoS attacks have served as a disguising maneuver for other types of attacks, such as attempts to penetrate or successful penetrations of systems.

2.2 Global trends

Infection by ransomware has the greatest impact on functioning of individuals and organisations.There is visible continuance of activities of professional gangs providing ransomware as a service.

The input vector to the systems is in most cases leakage or acquisition of credentials or a VPN of one of the companies’ employees (further supported by the trend towards home office), exploiting vulnerabilities in devices or freely available systems on the internet.

Innovations in ransomware malicious code are notable in upgrades to the functions (e.g. increased encryption speed, better data exfiltration masking). Leaked date at the beginning of 2022 have helped significantly in the fight against ransomware Conti ransomware communications which highlighted the modus operandi of the hacker groups (e.g. hierarchy structure, processes used and procedures). Successful gangs have also used to change their names to confused the law enforcement.

A ransomware attack is usually carried out manually, and while mapping the victim's system, the attacker can also gain access to vendors' systems (in a few cases, even those better secured), which can transform into supply chain attacks.

The most significant entry vector into the company's network continues to be phishing in various forms. A message arrives asking for password verification, which redirects the recipient to a website under the control of the attacker. In targeted spearphishing attacks, the website may look like or resemble an exact copy of the login site to which the victim is accustomed. To increase the similarity, attackers exploited, for example, a simple phishing tool called "Logo Kit" that personalized the login screen based on the victim's email address (taking the domain logo extracted from the victim's email address). A more recent theme in 2022 was the use of decentralized/shared networks to host phishing content – e.g., IPFS networks. Attackers have also started to use this approach ever since cloud storage providers have started to offer IPFS services.

URL shorteners continue to be exploited to bypass security features. While URL shorteners can be blocked with security features (automatic removal of email content), they are so popular and so widely used that companies do not prefer this method of security and focus on blocking and reporting specific URLs in their incident response processes.

Attackers have exploited current geopolitical events as narratives for phishing campaigns, similar to what they have done in the past. The themes of refugees and Russia's war against Ukraine were mostly exploited.

Regarding social engineering, deep fake technology has moved forward. It came to the attention of society after the creation of a fake video of President Zelensky calling for military surrender.

In Russia's war against Ukraine, social engineering was also used as a method of obtaining data for technical analysis and combat operations (e. g. Ukrainian agents, under the pretext of offering sexual services, demanded Russian soldiers to send photos, which were then located and used for precision missile attacks).

A significant change in the field of social engineering was cause by releasing the Chat-GPT in November, which cybercriminals have started to exploit to create phishing emails. SEO optimisation of phishing sites also continues to be used, with attackers trying to get to the top of search engines such as google.com and duckduckgo.com (so-called SEO poisoning). Pay-per-click ads have also been abused to push phishing or malicious content websites to the top of a given search engine. During malvertising campaigns, attackers misused the identity of popular tools and platforms such as the Brave browser, the uTorrent torrent client or the Audacity music hosting service.

In addition to input vectors, which include phishing, misconfiguration and vulnerabilities, there was increase of the creation of malicious programming libraries with names similar to legitimate ones (library typosquatting).

A high number of accounts thefts on various platforms were carried out through so-called password spraying. The primary problem remains that users do not enable two-factor or multi-factor authentication. In addition to the vulnerabilities that can be used to bypass two and multifactor autentification, the bombardment of access confirmation prompts (so-called MFA bombing) remains a threat. This approach consists of repeatedly sending two-factor authentication confirmation prompts. The attacker relies on inattention, exhaustion, or a simple click-through by the victim, or the victim is spammed until he or she succumbs to the coercion.

Microsoft changed the basic settings of its Office products in the middle of the year to not allow macros. This change forced attackers to switch to other formats – LNK, ISO and RAR. For example, an innovative attack was carried out by the APT group Gamaredon, which, while infecting the victim's device, rewrote the pattern of a new document in MS Word (Normal.dotm) so that every other document created on the victim's computer would spread the same malware.

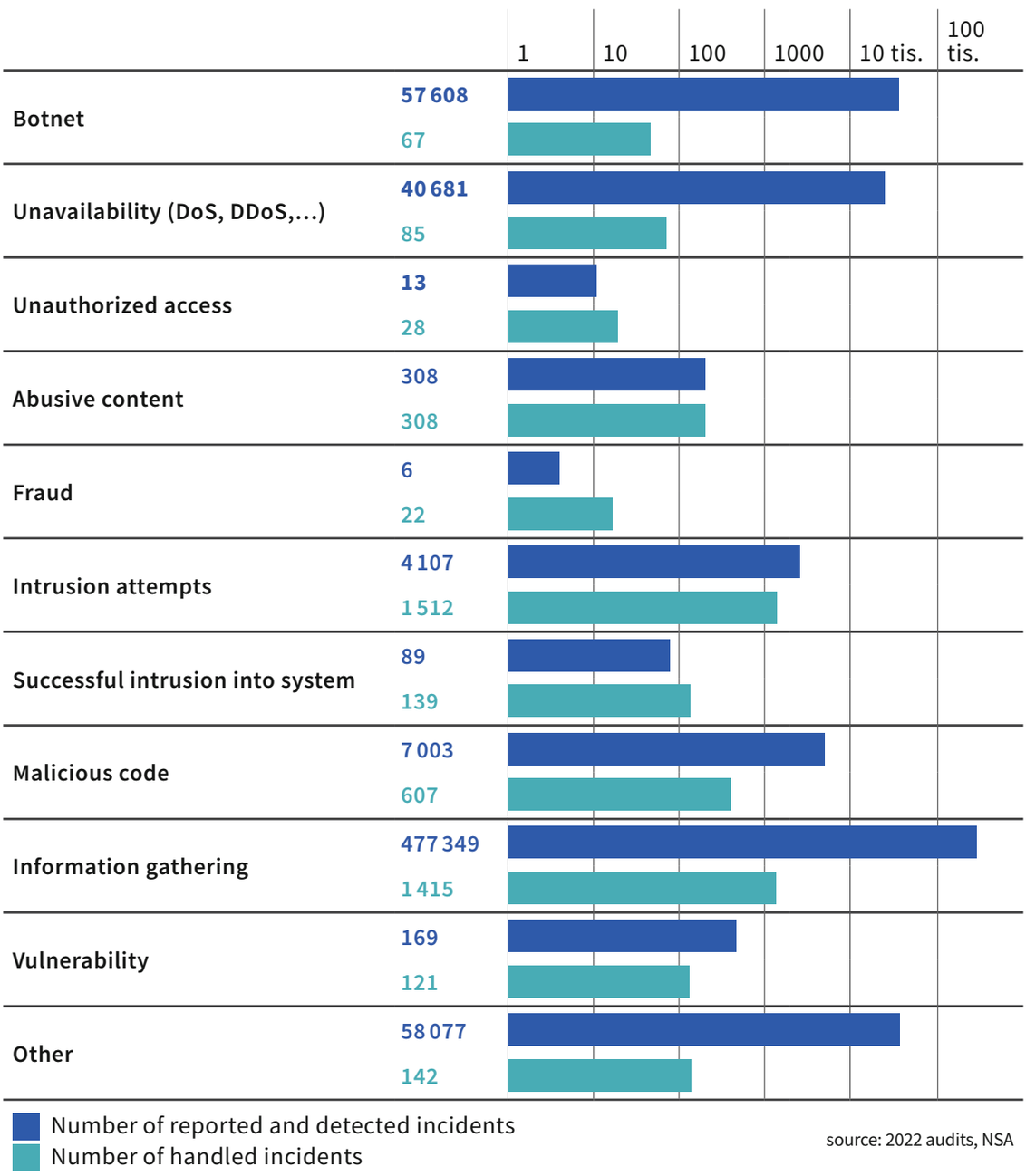
The most serious vulnerabilities in 2022 are those that have been actively exploited by attackers. Examples of these vulnerabilities include Log4Shell/Log4j (CVE-2021-44228), vulnerabilities in Google Chrome (CVE-2022-0609), ProxyNotShell (CVE-2022-41040 and CVE-2022-41082), vulnerabilities allowing remote code execution in Microsoft Exchange and Zimbra (CVE-2022-27925 and CVE-2022-41352), and vulnerability in Adobe Commerce (CVE-2022-24086).

2.3 Statistics of incidents in 2022

The National Cyber Security Centre SK-CERT, as a specialised unit of the Authority, continued to monitor the Slovak cyber space in 2022. It collected, analysed and evaluated the information obtained and received reports of cyber security incidents.

Based on the information obtained from self-detection, mandatory reporting from operators of essential services and digital service providers, voluntary reporting from Slovak companies, private individuals and partners and partner organisations, a comprehensive view of the number of incidents detected, reported and resolved in 2022 by incident type can be created.

Number of incidents detected, reported and resolved in 2021 by incident type

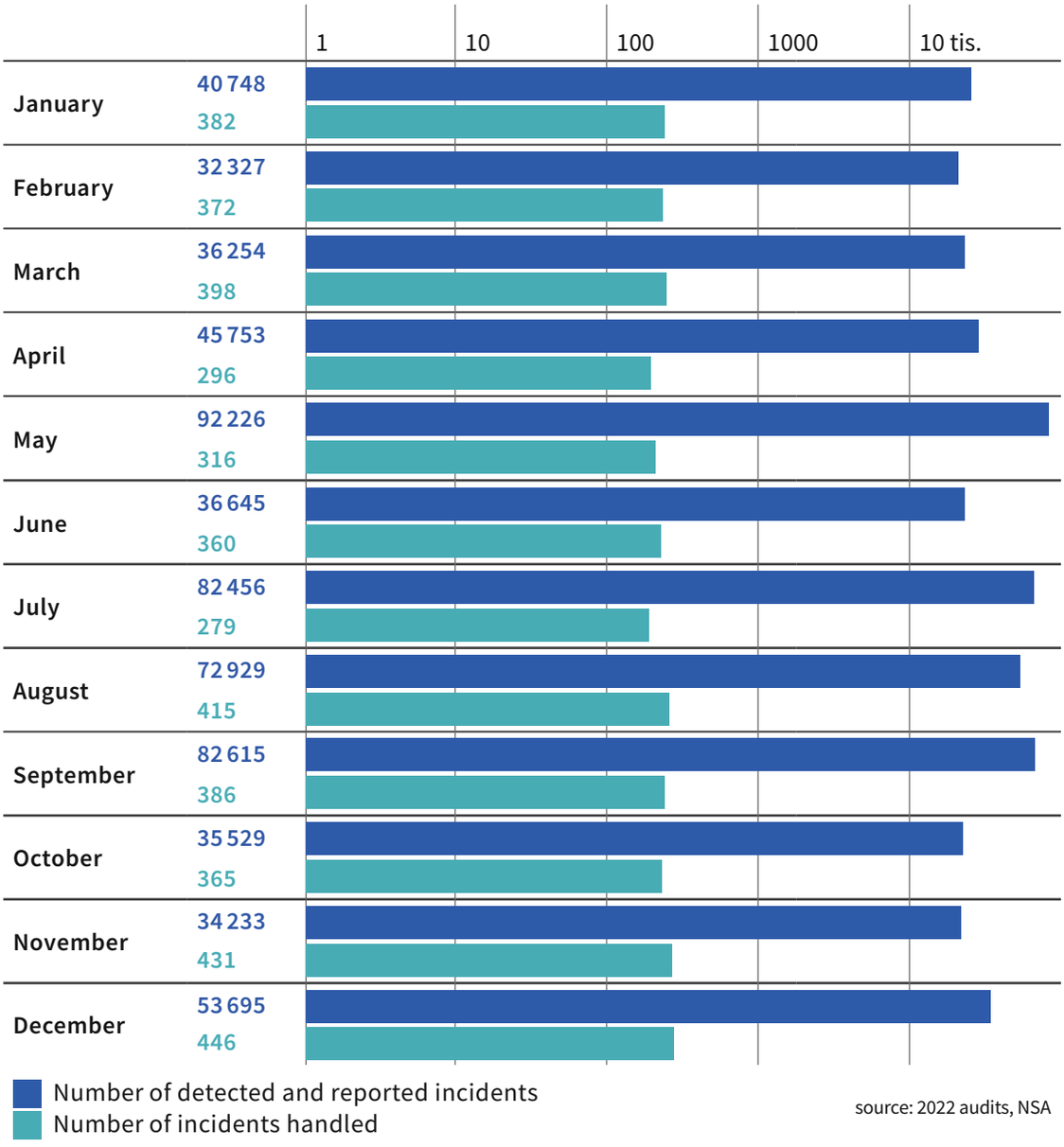


source: 2022 audits, NSA

The graphical display of statistics does not include incidents in the Abusive content category that were detected based on signatures through security scans. There were 48,887,103 potential incidents in this category all year around.

In terms of time, most incidents were detected and reported during May. The highest number of incidents resolved was in December.

Incidents over time – 2022

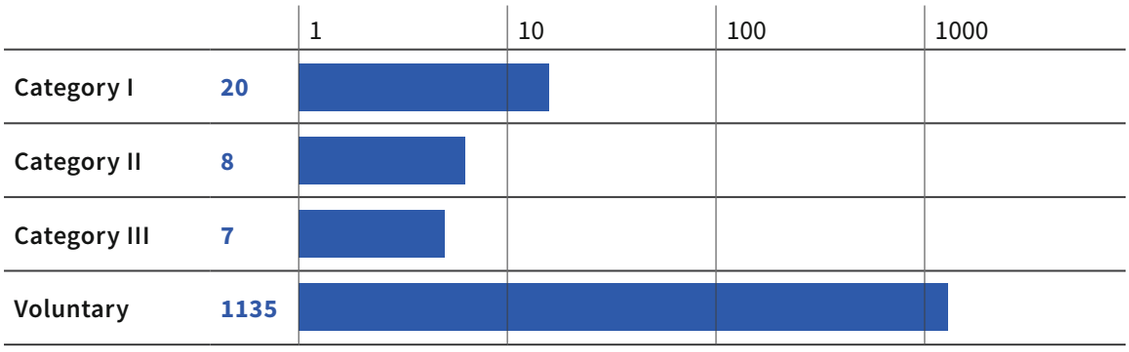


source: 2022 audits, NSA

OESs and DSP are legally obliged to report any serious cyber security incident. In 2022, we saw a 28% year-on-year increase in reporting, but this was mainly an increase in voluntary reporting of cybersecurity incidents. We consider it essential that providers in both groups focus more on this legal obligation as we still consider compliance to be inadequate, particularly in the most vulnerable sectors.

Weaknesses are also evident in the misclassification or lack of classification of cyber security incidents under the Cybersecurity Act. The problems with reporting cyber security incidents stem mainly from attempts by obliged entities to avoid or simplify their obligations under the law, but also from inadequate or non-existent monitoring, neglected or non-existent processes, or the complete absence of cyber security management in the organisation, or ignoring these issues.

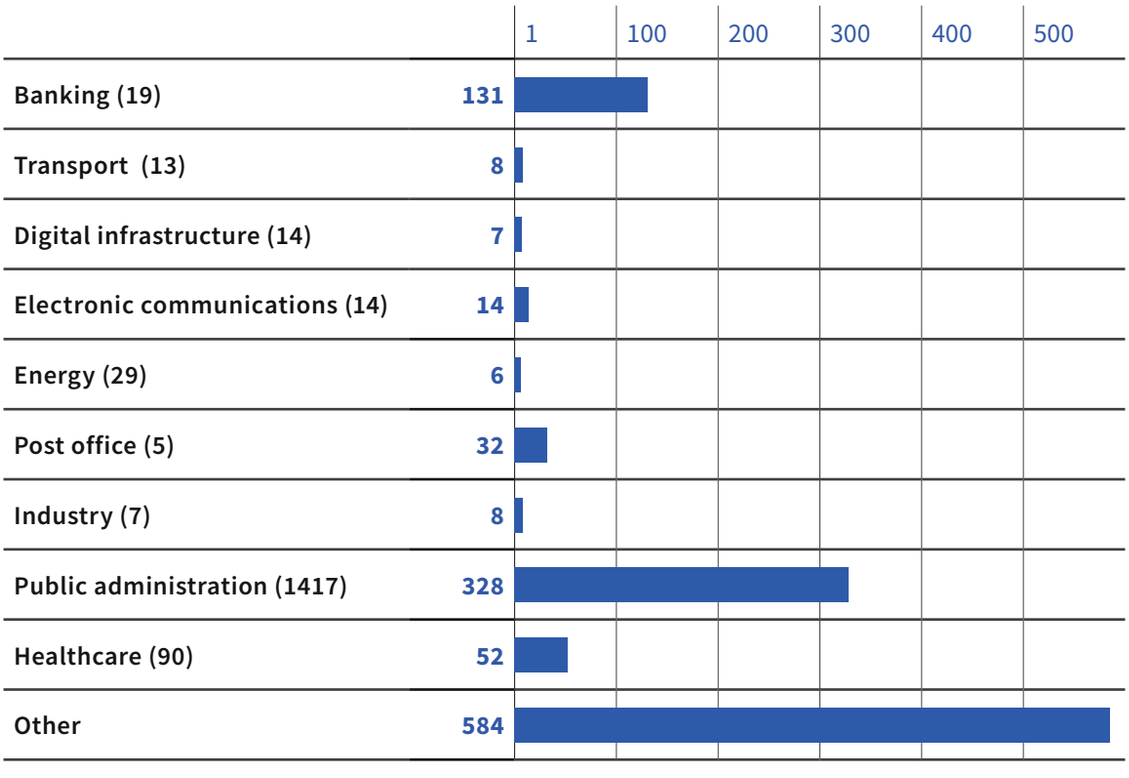
Number of cyber security incidents reported under the Cybersecurity Act – 2022



source: 2022 audits, NSA

The largest number of mandatory and voluntary reports within sectors was recorded in the sector of Public administration. In some sectors (Infrastructure of financial markets, Water and air), the National Cyber Security Centre SK-CERT did not receive any reports. The category “Other” includes voluntary reports from entities (companies, citizens) that were not classified in any of the sectors according to the law. The number of identified CERTs in the sector is indicated in brackets.

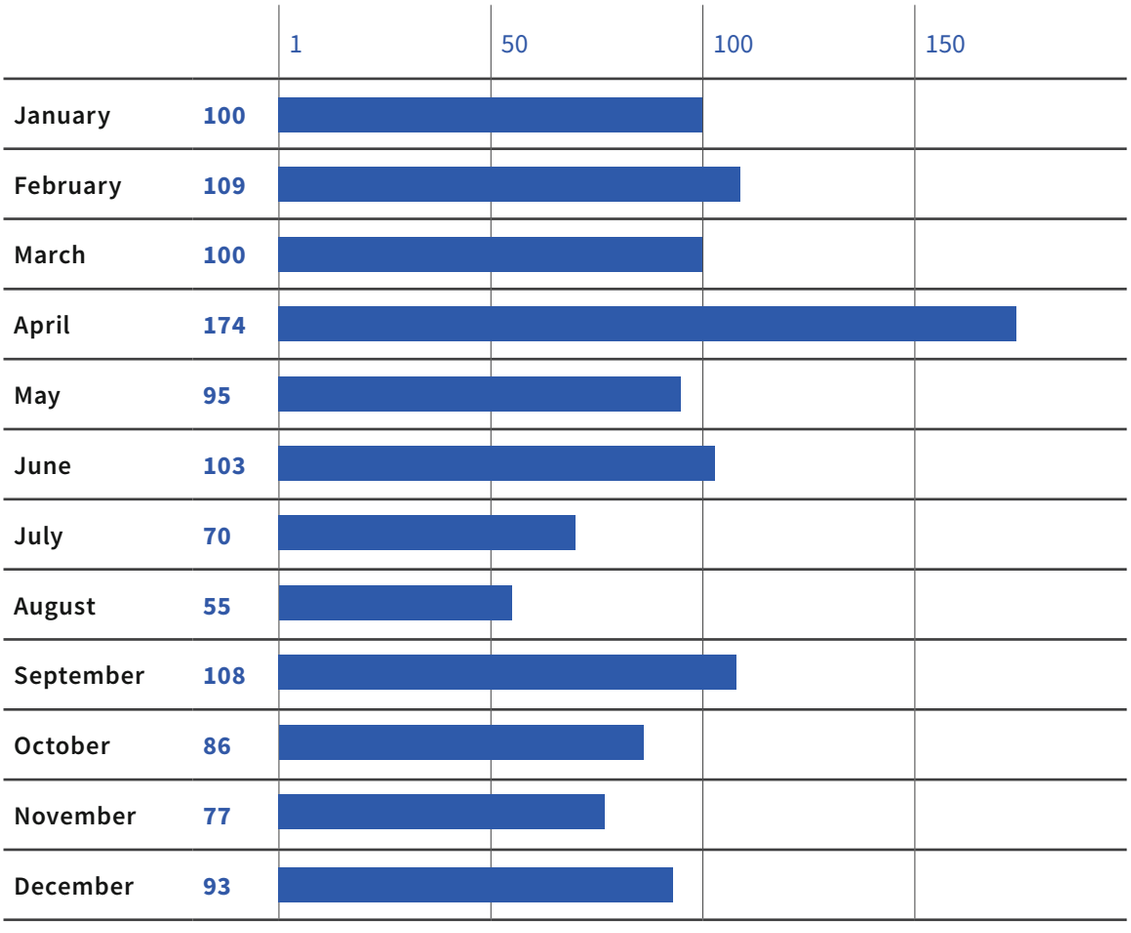
Cyber Security Incident Reports by Sector – 2022



source: 2022 audits, NSA

In terms of time, most incidents were reported in April.

Cyber Security Incident Reports by Sector – 2022



source: 2022 audits, NSA

2.4 The most significant threats in the Slovak Republic in 2022

2.4.1 SOCIAL ENGINEERING

Phishing campaigns (email, phone and SMS) imitating financial, email, web hosting and ISP services persisted throughout the year. Misuse of global supplier company brands (including postal services) was also common, with attacks varying in sophistication to the point where they plausibly replicated the communication style and design of the company whose name they were misusing. The attacker can benefit from the attack even more if he manages to gain access to a high-profile individual's work email account and then exploits this access for further attacks (a type of "Business email compromise" attack).

Phishing attacks continued to be used for obtaining login and other sensitive data and to spread malicious code. A significant change was that attackers exploiting malicious macros in MS Office email attachments switched to alternative attachment formats (e.g. LNK, ISO and RAR) after Microsoft changed the underlying configurations (disabling macros).

In September, there were acknowledged the first reports of telephone and e-mail phishing campaigns exploiting the identities of law enforcement agencies, Interpol and Europo. Most of the reported

telephone campaigns were conducted in English, the victims were contacted repeatedly and the form of communication was gradually getting more aggressive. The e-mail campaigns were of poor quality (the e-mails were poorly processed) and contained an "official looking" MS Word document.

Also in 2022, some attackers targeted fraudulent activity on advertising portals. The attack method did not change – the seller was approached by an attacker who, under the pretext of ordering transport, he planted a malicious URL into which the victim subsequently entered his payment card details.

Various pyramid schemes related to cryptocurrency investments have also been reported. The fraudulent scheme aims to extort as much money as possible from the victim, and in order to appear credible, the attacker pays a real commission or return to the victim at the beginning, but stops at a certain point, while the victim is still mostly invested. These concepts have massive advertising, for example on social media.

2.4.2 UNAVAILABILITY OF SERVICE, DDOS ATTACKS

In general, a distinction can be made between unavailability due to an attack and unavailability due to an unexpected phenomenon or operational failure. From the perspective of the Slovak cyberspace, the most frequent unavailability of the service was caused by operational reasons – post-update problems, various accidents, misconfigurations and inadequate response of administrators to increased web traffic, which was interpreted as a DDoS attack.

DDoS attacks related to Russia's war against Ukraine were also prominent. In February, some Slovak media were targeted by activist DDoS attacks. The attacks mostly used freely distributed tools, but they were also spread by websites that performed DDoS via their visitors' browsers (even without their knowledge).

In April, large-scale DDoS attacks on NATO member states by the community hacking groups LEGION and KILLNET were reported. Further KILLNET attacks were recorded in June and October, to which the group Anonymous Russia has confessed. In most cases, individual groups have publicly admitted to DDoS attacks.

Most of the attacks were carried out from IP addresses belonging to TOR anonymization services, VPN services, open proxy services and compromised devices that were part of the infrastructure of DDoS tools, which attackers rented as a service on the black market.

The most visible DDoS attacks in Slovak cyberspace were aimed at denying access to various websites and services of various public institutions (ministries), as well as private companies (banks, airports, transport companies). These attacks were coordinated and among targets were EU and NATO Member States and their public institutions or other important organizations. The attacks were often in response to statements by public officials or to the approval of specific sanctions imposed against Russia.

2.4.3 MALICIOUS CODE

May, June and November saw an increase in Emotet malware activity. Activity was reflected in reported phishing campaigns and from information coming from foreign partners.

In October, November and December, several campaigns were reported that spread SystemBC malware (mostly leading to ransomware infections). Similarly, other malware activities were recorded during 2022, such as Trickbot, Ursnif, Systembc, Hajime, Mirai, Expiro Gazavat, IcexLoader and others, including ransomware (HIVE, Venus, PLAY, Lockbit, Bozq and mig21 and others).

The most common vectors of malicious code infection were successful social engineering attempts, poor security management (using private devices for work purposes, using business accounts for private purposes, etc.), visiting compromised websites, installing illegal software, and exploiting existing vulnerabilities on devices accessible from the Internet.

2.4.4 VULNERABILITIES AND INTRUSIONS

The most common entry vector into victims' systems are still phishing attacks, or inattentiveness of employees, when they decide to fill in application on the website which are actually phishing websites. Still critical there are also incorrect device configurations – open RDP, FTP and available login interfaces which attackers identify by continuous scanning.

Also, published instructions for exploiting vulnerabilities are within a few hours used by attackers when they immediately scan their targets. During the year they were (based on information available from public sources) performed tailor-made alerts that contained information about incorrectly configured devices, about potential data leaks and vulnerabilities (e.g. publicized vulnerabilities in MS Exchange, QNAP NAS, Fortinet and Zimbra). Attackers are also conducting brute-force attacks, for example password spraying. Several incidents were caused incorrect password usage policy, e.g. by repeatedly using passwords that are already (often years) compromised or were just set by default.

Organizations use dozens of different technologies and their maintenance is difficult and time-consuming due to the smaller number of teams. The absence of policy of regular updates often causes conflict of interests – availability of services during operating hours hours and working time of the employee, what leads to the necessary use of long-term non-updated ones technologies. Absence of asset management causes that by changing the managing IT employee forgets less used technologies and does not they continue to be maintained and updated.

2.4.5 DATA EXPENDITURE

The National Cyber Center of Cyber security SK-CERT identified several compromised e-mail accounts and RDP accesses, which were offered for sale on hacker forums (victims were warned). There was also extended cooperation with the banking sector, which was regular informed about potential compromises payment cards. One of the identified of leaks was the payment card database which was shared for free by hacking store BidenCash as part of its marketing.

3 SECTOR VIEW

The main source of data for assessing the sectoral view are not only the results of audit reports, but also the assessments of the activities of individual central authorities. It can be concluded that the condition of cyber security varies considerably from sector to sector.

The "**Banking**" sector continuously shows a very good performance in the area of cyber security. The OESs approach this topic responsibly not only in implementing security requirements but also in communicating with the NSA. They react promptly and very quickly when dealing with incidents and other problems. The representatives of the OESs in this sector are also active in building the security community.

Entities in the "**Healthcare**" sector are gradually improving their perception of the topic of cyber security. This is facilitated by the improving quality of activities of its central authority. The gradual realisation of responsibility not only for data but also for ensuring the functionality of systems and services on which human lives depend is gradually improving the state of cybersecurity in this sector.

The "**Energy**" sector has the most pronounced difference between the sub-sectors and in the sub-sectors themselves. The '**Gas industry**' sub-sector performs best among all sectors and sub-sectors in terms of audit results. In the case of the **Electrical power** sub-sector, there are significant differences between the different OESs. In contrast, the '**Thermal energy**' sub-sector continues to have extremely poor audit results, despite the fact that it is an important sub-sector whose operation has a very large impact on the daily life of citizens, especially in winter. A reduction or interruption of services can have a major impact on people's lives and health.

For the sectors "**Infrastructure of financial markets**", "**Industry**" and "**Post office**" it is not possible to get a clear picture of the state of cyber security. The central authorities responsible for these sectors have not provided specific information on the conditions of cybersecurity in these sectors, and there are not enough audit reports submitted in these sectors to provide a sufficiently anonymised statistical sample.

In the "**Public administration**" sector, sub-sector" **Public administration information systems**", where the largest number of OESs is located, the situation in the field of cyber security has not changed in the long term. There is still an almost critical neglect of cyber security. In particular, municipalities and smaller entities are not sufficiently aware of the importance of the topic of cyber security, they approach the issue superficially and focus rather on fulfilling formal activities (e.g. buying universal security documentations).

They also often seek to outsource the responsibility for dealing with these issues, including responsibilities that belong only to the company's statutory body and are therefore non-transferable. Overall cybersecurity governance of OESs in this sector is often lacking, chaotic or only particular. However, these findings does not apply only to municipalities or small operators, but also to some of the large OESs in this sub-sector, including government institutions.

3.1 Significant findings in audits

From the audit reports submitted by OESs in 2022, the following are the most frequent findings (regardless of sector):

3.1.1 CYBER SECURITY MANAGEMENT

- Non-existent cyber security strategy and lack of top management support
- Unspecified manager of cyber security, eventually non-formal work position
- There is no defined structure of governance, execution and control in the area of cyber security
- Management control mechanisms are not defined
- Independence of cyber security management from IT management is not guaranteed
- Serious weaknesses in management of assets, threats and risk management
- There is no responsibility for the identification and registration of assets
- Rules and responsibilities for the implementation of the measures are not established
- Information classification and categorisation of information systems is not carried out
- Insufficient, outdated or missing security documentation
- No documented security architecture or definition of the scope and implementation of security measures
- There are no or no updated guidelines containing physical security requirements
- Rules described in policies are not put into practice (low maturity of processes)
- Business impact analyses are not carried out
- No specific HR practices are defined in relation to cyber security
- Procedures for the assignment of persons to security roles, their competences and remits are not defined
- Responsibilities in regard to cyber security are not part of employment contracts
- The principle of least privilege is not established
- The principle of distinction of responsibilities is not established
- Procedures are not established for the transfer of competencies, duties and responsibilities in relation to cyber security to another person
- There are no formalised exit management processes for security roles
- Contracts with suppliers do not include cyber security principles
- Processes for independent evaluation, measurement and review of the effectiveness and efficiency of the security measures are not identified
- There is no audit programme in place that includes IT and security controls
- Lack of training in information security and data protection

3.1.2 IMPLEMENTATION OF SECURITY MEASURES

- Operational records are not kept
- No tool for monitoring of incidents is implemented
- Missing topology, segmentation, port lists
- Inadequate cryptographic information protection solutions
- There is no backup communication path for connectivity
- No access control policy implemented
- There is no formally defined process for handling and reporting security incidents
- Absence of business continuity management processes
- Contingency and continuity plans are not tested
- Backup plans and backup requirements are not prepared
- Unclear and not official backup procedures
- Backup recovery testing is not performed
- Remote access is not provided (applies to both employees and contractors)
- There is no solution implemented for automatic security authentication of third-party devices
- Secure software development lifecycle (SSDLC) processes are not specified

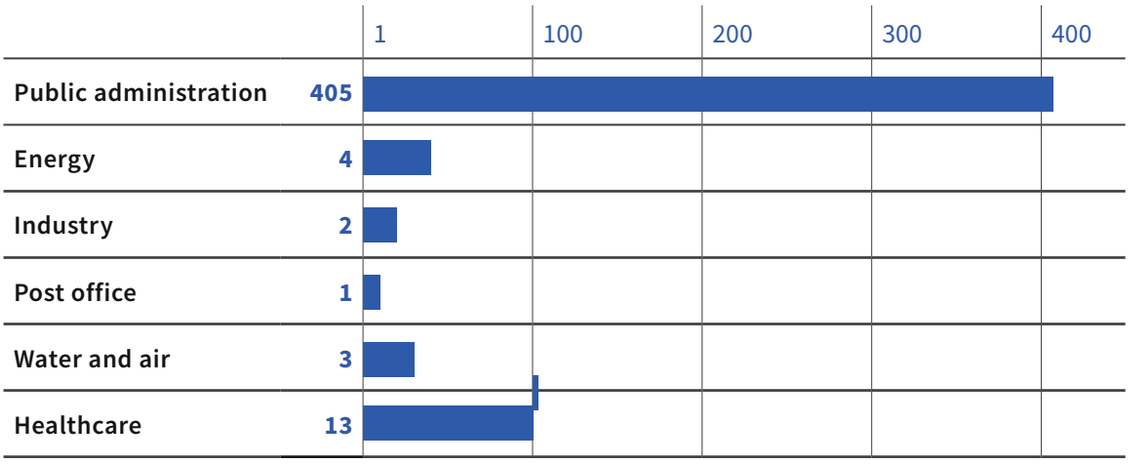
3.2 Self-assessments

The degree of implementation of legal requirements in the area of cyber security can also be verified by the so-called self-assessment executed by the cyber security manager. The self-assessment fully replaces the requirement of a cybersecurity audit and can only be carried out by the OESs in Categories I and II of networks and information systems in the period from 1 August 2021 to 31 December 2023.

The NSA has published a self-assessment form on its website, which is made up of a series of questions in order to determine the level of cyber security at the OESs.

As of 31 December 2022, the NSA had received 428 self-assessments, when majority of them comes from the Public Administration sector (405 self-assessments).

Number of cyber security incidents reported under the Cyber security Act – 2022



source: 2022 audits, NSA

3.3 Sanctions

According to Act No. 69/2018 on Cyber Security, the Authority is entitled to impose a fine if the OES breaches its obligations under this Act. In 2022, the Authority carried out a number of inspections of compliance with the legal obligations by the operators of the essential services. The Authority fined two entities a total of 26 000 EUR.

3.4 Banking

Central authority: the Ministry of Finance of the Slovak Republic (MoF SR)

Number of OESs: 19

Number of OESs with audit obligation in 2022: 18
(can also be fulfilled by self-assessment according to §34a (2) of Cyber security Act)

Number of audit reports submitted: 13

Number of self-assessments submitted: 0

Subsectors: none

3.4.1 ASSESSMENT OF THE STATE OF CYBERSECURITY IN 2022 BY THE CENTRAL AUTHORITY

3.4.1.1 Threats

According to the MoF, the most significant threats in 2022 were advanced persistent threats (APTs), ransomware attacks, growing attacks on the Internet of Things (IoT), security threats in the cloud (related to the growing number of organisations moving their data and applications to the cloud) and social engineering attacks.

3.4.1.2 Activities

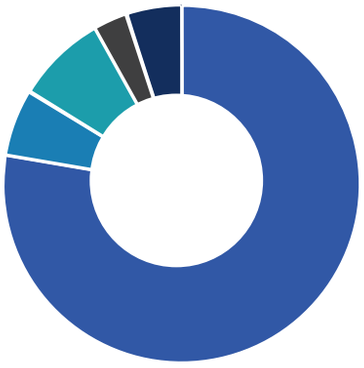
During 2022, the MoF, as the central authority within the meaning of Act No. 45/2011 on Critical Infrastructure, carried out an inspection of the operators of the Finance sector element within the meaning of Section 9 “Obligations of the operator”. During the inspection activity, deficiencies were identified in some entities, which they were called upon to correct, while the MoF SR provided recommendations for upgrading processes of protection of the operator from disruption or destruction, completion of security documentation, performance of related audits and others in accordance with the applicable legislation. The MoF has started to build a Security Operations Centre (SOC) as a specific department of the Ministry, and in December 2022, the MoF SOC became a member of the international TF CSIRT association under the status of a “Listed team”.

3.4.1.3 Plánované aktivity

The MoF plans to develop a mechanism for training its staff in the fight against cyber threats (e-learning portal LMS, internal training of employees). It also plans to accredit the SOC Security Monitoring Unit within the international association TF CSIRT. In addition, it plans to organise a meeting with representatives of the sectoral organizations of the Ministry of Finance in the order to improve the services provided in cyber security, initially as a pilot project to kick-off exchanging relevant information on cyber attacks and sending relevant warnings.

3.4.2 RESULTS OF OESS AUDITS IN THE BANKING SECTOR

As of 31.12.2022, the National Security Authority had received a total of 13 audit reports from the Banking sector (unchanged from 2021). Not all operators must carry out an audit, because in cases under the law some of them can choose to deliver self-assessments, which are not included in this statistic. Based on statistics on compliance with audit requirements, in the Banking sector the average percentage compliance rate as follows:



Average percentage compliance rate (year 2022)

FULL COMPLIANCE	77 %
PARTIAL COMPLIANCE	6 %
NON-COMPLIANCE	8 %
NOT APPLICABLE	3 %
VERIFIED ELSEWHERE	5 %

Looking at individual OESs in the Banking sector, the high level of compliance with audit requirements is present across all operators. The highest compliance rate was achieved by one of the OESs, which out of 226 audited requirements, achieved compliance in 218 requirements and partial compliance in 8 requirements. On the other hand, the lowest compliance rate was identified for the OES, which out of 264 audited requirements achieved compliance in 66 requirements and non-compliance in 153 requirements (15 requirements were not applicable, 12 were verified elsewhere).

3.4.3 MOST FREQUENT AUDIT FINDINGS

The most frequent audit findings in the Banking sector include:

- there is no documented definition of the extent and methods of implementation of all security measures,
- there are no procedures for the transfer of competencies, duties and responsibilities in relation to cyber security to another person,
- Input-output points are identified only in the relevant documentation for individual projects, and there is no overall list,
- third-party device controls are not implemented.

3.5 Transport sector

Central authority: the Ministry of Transport of the Slovak Republic (MoT SR)

Number of OESs: 13

Number of OESs with audit obligation in 2022: 13
(can also be fulfilled by self-assessment according to §34a (2) of Cyber Security Act)

Number of audit reports submitted: 9

Number of self-assessments submitted: 0

Subsectors: air transport, rail transport, road transport, water transport

3.5.1 ASSESSMENT OF THE STATE OF CYBERSECURITY IN 2022 BY THE CENTRAL AUTHORITY

3.5.1.1 Threats

The most serious threats identified by the MoT SR were lack of professional personnel capacity for security, threats of social engineering, threats related to the increased number of various types of attacks related to the military conflict in Ukraine and the obsolescence of hardware and software.

3.5.1.2 Activities

The MoT SR carried out an analysis of the needs and requirements of the transport, postal and electronic communications sectors, which belong under its responsibility. As the result of the analysis, the sectoral criteria were updated. They are the starting point of the preparation for the drafting of sectoral decrees defining sectoral security measures for individual sectors. On the basis of the analysis of the sectoral criteria in the context of NIS 2, the MoT SR identified the requirements which will subsequently be modified in the sectoral decrees in the framework of the transposition of the NIS 2 requirements.

3.5.1.3 Planned activities

The MoT SR plans to transpose the requirements of NIS 2 into the national legislation of the Slovak Republic with the determination of competences between the concerned sectors, including the preparation of sectoral decrees for the transport sector, the postal sector and the electronic communications sector.

3.5.2 RESULTS OF OES AUDITS IN THE TRANSPORT SECTOR

As of 31.12.2022, the National Security Authority has received a total of 9 audit reports from the Transport sector. Not all operators must carry out an audit, because in cases under the law some of them can choose to deliver self-assessments, which are not included in this statistic. Based on the audit compliance statistics, in the Transport sector, the average compliance percentage is as follows:

Average percentage compliance rate (year 2022)

FULL COMPLIANCE	46 %
PARTIAL COMPLIANCE	17 %
NON-COMPLIANCE	28 %
NOT APPLICABLE	3 %
VERIFIED ELSEWHERE	5%

source: 2022 audits, NSA

In the Transport sector, the average compliance rate is below 50%. The highest compliance rate was achieved by the OES, which achieved compliance in 205 out of 266 audit requirements, partial compliance in 17 requirements and non-compliance in 14 requirements (15 requirements were not applicable and 15 were verified elsewhere).

The lowest compliance rate was achieved by the OES, which achieved compliance in 20 out of 261 audit requirements, partial compliance in 68 requirements and non-compliance in 156 requirements (5 requirements were not applicable, 12 were verified elsewhere).

3.5.3 MOST FREQUENT AUDIT FINDINGS

The most frequent audit findings in the Transport sector include:

- roles and responsibilities in the area of cyber security are not sufficiently defined,
- A cybersecurity manager is not appointed,
- Control mechanisms in the area of cybersecurity management are not defined,
- Contracts with suppliers do not contain all the mandatory elements required by Decree 362 and are not in the central register,
- no access management policy is defined and implemented.

3.6 Digital infrastructure

Central authority: the National Security Authority (NSA)

Number of OESs: 14

Number of OESs with audit obligation in 2022: 14
(can also be fulfilled by self-assessment according to §34a (2) of Cyber Security Act)

Number of audit reports submitted: 11

Number of self-assessments submitted: 0

Subsectors: none

3. 6. 1 ASSESSMENT OF THE STATE OF CYBERSECURITY FOR 2022 BY THE CENTRAL AUTHORITY

3.6.1.1 Threats

The NSA has identified in the Digital Infrastructure sector the same significant threats which frequently occur within Slovak cyberspace – attacks using social engineering (especially phishing and vishing), spreading malicious code and exploiting vulnerabilities.

Further, a significant threat to the Digital Infrastructure sector is the misuse of compromised OES´s infrastructure to carry out other attacks (botnet management, DoS attacks, propagation ofphishing, spreading malicious code).

3.6.1.2 Activities

V In the Digital Infrastructure sector, the NSA carries out a number of activities, the most important of which is coordinating the handling of cyber security incidents. It also performs preventive-activities in the form of early warnings and the sending of relevant information to the sector's entities and also provides regular expert advice to individual OESs as required.

3.6.1.3 Planned activities

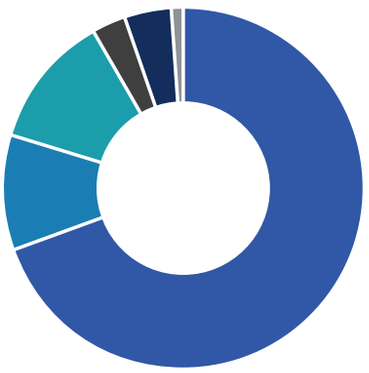
The NSA plans to continue its existing activities and gradually improve its tasks for securing OESs. The NSA regularly reviews the situation in the Digital Infrastructure sector and in will respond flexibly if necessary.

3. 6. 2 RESULTS OF THE AUDITS OF THE OESS IN THE DIGITAL INFRASTRUCTURE SECTOR

The National Security Authority has received a total of 11 audit reports from the Digital Infrastructure sector as of 31.12.2022. Not all operators must carry out an audit, because in cases under the law some of them can choose to deliver self-assessments, which are not included in this statistic Based on the audit compliance statistics, in the Digital Infrastructure sector, the average compliance percentage is as follows:

Looking at OESs in the Digital Infrastructure sector, compliance with audit requirements is more than half for the majority of operators, which is reflected in the overall compliance rate in the sector. The highest compliance rate was achieved by the OES which was compliant in 157 requirements out of 162 audit requirements, partially compliant in 3 requirements and had no non-compliance in any of the requirements (the other requirements were not applicable).

On the other hand, the lowest compliance rate was identified for the OES which, out of 273 audit requirements, achieved compliance in 94 requirements, partial compliance in 28 requirements and non-compliance in 117 requirements (13 requirements were not applicable, 21 were verified elsewhere).



Average percentage compliance rate (year 2022)

FULL COMPLIANCE	69 %
PARTIAL COMPLIANCE	10 %
NON-COMPLIANCE	12 %
NOT APPLICABLE	3 %
VERIFIED ELSEWHERE	4 %
UNEXPECTED	1 %

source: 2022 audits, NSA

3.6.3 MOST FREQUENT AUDIT FINDINGS

The most common audit findings in the Digital Infrastructure sector include:

- there are no defined procedures for assigning persons to security roles with clearly defined responsibilities and authorities,
- regular risk analysis is not carried out,
- Cyber security management continuity requirements are not identified,
- backup plans are not in place,
- testing of contingency plans is not carried out.

3.7 Electronic communications

Central authority: the Ministry of Transport of the Slovak Republic (MoT SR)

Number of OESs: 11

Number of OESs with audit obligation in 2022: 11
(can also be fulfilled by self-assessment according to §34a (2) of Cyber Security Act)

Number of audit reports submitted: 9

Number of self-assessments submitted: 0

Subsectors: satellite communications, networks and services of fixed and mobile electronic communications

3.7.1 ASSESSMENT OF THE STATE OF CYBERSECURITY IN 2022 BY THE CENTRAL AUTHORITY

3.7.1.1 Threats

The Central Authority has provided a threat assessment only for the Transport sector.

3.7.1.2 Activities

The MoT SR carried out an analysis of the needs and requirements of the transport, postal and electronic communications sectors, which belong under its responsibility. As the result of the analysis, the sectoral criteria were updated. They are the starting point of the preparation for the drafting of sectoral decrees defining sectoral security measures for individual sectors. On the basis of the analysis of the sectoral criteria in the context of NIS 2, the MoT SR identified the requirements which will subsequently be modified in the sectoral decrees in the framework of the transposition of the NIS 2 requirements.

3.7.1.3 Planned activities

The MoT SR plans to transpose the requirements of NIS 2 into the national legislation of the Slovak Republic with the determination of competences between the concerned sectors, including the preparation of sectoral decrees for the transport sector, the postal sector and the electronic communications sector.

3.7.2 RESULTS OF OESS AUDITS IN THE ELECTRONIC COMMUNICATIONS SECTOR

As of 31.12.2022, the National Security Authority has received a total of 9 audit reports from the Electronic Communications sector. Not alloperators must carry out an audit, because in cases under the law some of them can choose to deliver self-assessments, which are not included in this statistic. Based on the audit compliance statistics, in the Electronic communications sector, the average compliance percentage is as follows:

Average percentage compliance rate (year 2022)

FULL COMPLIANCE	73 %
PARTIAL COMPLIANCE	9 %
NON-COMPLIANCE	13 %
NOT APPLICABLE	2 %
VERIFIED ELSEWHERE	3 %

source: 2022 audits, NSA

Looking at individual OESs in the Electronic Communications sector, compliance with audit requirements is more than half across all operators. The highest compliance rate was achieved by the OES, which achieved a 100% compliance rate across all 199 audited requirements.

On the other hand, the lowest compliance rate was achieved by the OES, which out of 266 requirements audited, achieved compliance in 13 requirements, partial compliance in 44 requirements and non-compliance in 189 requirements (7 requirements were not applicable, 13 were verified elsewhere).

3.7.3 MOST FREQUENT AUDIT FINDINGS

The most common audit findings in the Electronic Communications sector include:

- Cybersecurity requirements throughout the lifecycle of information and IS are not taken into account,
- specific HR practices in relation to cyber security are not defined,
- Contracts with suppliers do not contain cyber security requirements,
- There were no established rules for working in the secure area of the OESs,
- Backup requirements are not formalised; backup documentation is not centrally registered by the OESs.

3.8 Energy

Central authority: the Ministry of Economy of the Slovak Republic (MoE SR)

Number of OESs: 29

Number of OESs with audit obligation in 2022: 28
(can also be fulfilled by self-assessment according to §34a (2) of Cyber Security Act

Number of audit reports submitted: 20

Number of self-assessments submitted: 4

Subsectors: mining, Electrical power, gas industry,
petroleum and petroleum products, Thermal energy

3.8.1 ASSESSMENT OF THE STATE OF CYBERSECURITY FOR 2022 BY THE CENTRAL AUTHORITY

3.8.1.1 Threats

According to the statement of the central authority, the MoE did not face any threats in sectors or sub-sectors in 2022.

3.8.1.2 Activities

In cooperation with other central authorities, the Ministry of Economy commented on the Cyber Defence Strategy of the Slovak Republic and the NSA Decree determining knowledge standards in the field of cyber security.

The representative of the Ministry of Economy participated in several working groups related to cyber security. No activities beyond §9(1)(c) of Act No. 69/2018 on cyber security were carried out.

3.8.1.3 Planned activities

For full coordination in the field of cyber security in the sectors and subsectors for which the MoE SR is responsible according to the law, the MoE SR plans to create a post for coordination of cyber security in sectors and subsectors, respectively for communication and coordination of cyber security with the OESs.

3.8.2 RESULTS OF THE ENERGY SECTOR AUDITS OF THE OESS

As of 31.12.2022, the National Security Authority has received a total of 20 audit reports from the Energy sector. Not all operators must carry out an audit, because in cases under the law some of them can choose to deliver self-assessments, which are not included in this statistic. Based on the audit compliance statistics, in the Energy sector, the average compliance percentage is as follows:

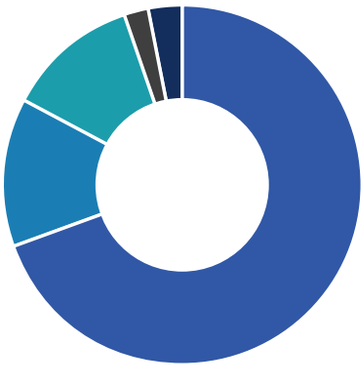
Average percentage compliance rate (year 2022)

FULL COMPLIANCE	57 %
PARTIAL COMPLIANCE	19 %
NON-COMPLIANCE	21 %
NOT APPLICABLE	2 %
VERIFIED ELSEWHERE	2 %

source: 2022 audits, NSA

In the Energy sector, large differences across sectors are present.

In the sub-sector of Electrical power, the compliance rate is almost 70%, and in the case of sub-sector of Gas industry it is almost 90%. In the Thermal Power sector, the average compliance rate is below 1%.



Electrical engineering – average percentage Compliance rate (2022)

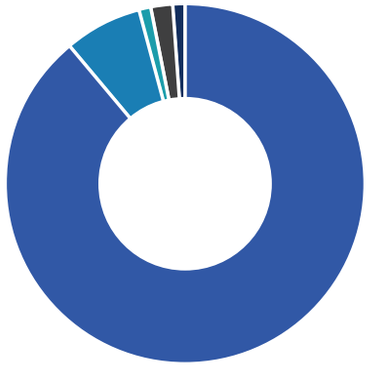
COMPLIANCE	69 %
PARTIAL COMPLIANCE	13 %
NON-COMPLIANCE	12 %
NOT APPLICABLE	2 %
VERIFIED ELSEWHERE	3 %

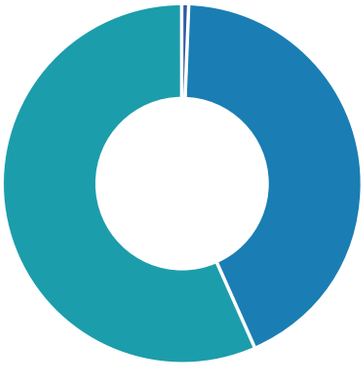
source: 2022 audits, NSA

Gas – average percentage Compliance rate (2022)

COMPLIANCE	88 %
PARTIAL COMPLIANCE	7 %
NON-COMPLIANCE	1 %
NOT APPLICABLE	2 %
VERIFIED ELSEWHERE	1 %

source: 2022 audits, NSA





Thermal energy – average percentage compliance rate (2022)

COMPLIANCE	0,8 %
PARTIAL COMPLIANCE	42,8 %
NON-COMPLIANCE	56,4 %

source: 2022 audits, NSA

In the case of the Thermal energy sub-sector, two operators achieved zero compliance with the audited requirements.

3.8.3 MOST FREQUENT AUDIT FINDINGS

The most common audit findings in the Energy sector include:

- the list of control activities in the company is not defined,
- the operator did not have an audit programme in place which would included IT and security controls,
- no business impact analysis has been carried out,
- processes for employment within security roles are not formalised,
- technical measures against malicious code are not applied for remote access for supply-chain end points.

3.9 Infrastructure of financial markets

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

Number of OESs: 1

Number of OESs with audit obligation in 2022: 1
(can also be fulfilled by self-assessment according to §34a (2) of Cyber Security Act)

Number of audit reports submitted: 1

Number of self-assessments submitted: 0

Subsectors: none

3.9.1 ASSESSMENT OF THE STATE OF CYBERSECURITY FOR 2022 BY THE CENTRAL AUTHORITY

The Central Authority sent the same assessment as for the Banking sector.

3.9.2 RESULTS OF AUDITS OF THE FINANCIAL MARKETS INFRASTRUCTURE SECTOR

Due to the impossibility of creating an anonymised statistical sample from a single operator, we do not present the result of its audit in this report.

3.10 Post office

Central authority: Ministry of Transport and Construction of the Slovak Republic

Number of OESs: 5

Number of OESs with audit obligation in 2022: 3
(can also be fulfilled by self-assessment according to §34a (2) of Cyber Security Act)

Number of audit reports submitted: 1

Number of self-assessments submitted: 1

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

3.10.1 ASSESSMENT OF THE STATE OF CYBERSECURITY FOR 2022 BY THE CENTRAL AUTHORITY

3.10.1.1 Threats

The Central Authority provided a threat assessment only for the Transport sector.

3.10.1.2 Activities

The MoT SR carried out an analysis of the needs and requirements of the transport, postal and electronic communications sectors, which belong under its responsibility. As the result of the analysis, the sectoral criteria were updated. They are the starting point of the preparation for the drafting of sectoral decrees defining sectoral security measures for individual sectors. On the basis of the analysis of the sectoral criteria in the context of NIS 2, the MoT SR identified the requirements which will subsequently be modified in the sectoral decrees in the framework of the transposition of the NIS 2 requirements.

3.10.1.3 Planned activities

The MoT SR plans to transpose the requirements of NIS 2 into the national legislation of the Slovak Republic with the determination of competences between the sectors concerned, including the preparation of sectoral decrees for the transport sector, the postal sector and the electronic communications sector.

3.10.2 RESULTS OF AUDITS OF THE POSTAL SECTOR

Only one audit report was submitted in the sector of Post Office, therefore it is not possible to produce an anonymised assessment of the results of the sector audits.

3.11 Industry

Central authority: the Ministry of Economy of the Slovak Republic (MH SR)

Number of OESs: 7

Number of OESs with audit obligation in 2022: 7
(can also be fulfilled by self-assessment according to §34a (2) of Cyber Security Act)

Number of audit reports submitted: 2

Number of self-assessments submitted: 2

Subsectors: pharmaceutical industry, metallurgical industry, chemical industry

3.11.1 ASSESSMENT OF THE STATE OF CYBERSECURITY FOR 2022 BY THE CENTRAL AUTHORITY

3.11.1.1 Threats

According to the statement of the central authority, the MoE did not face any threats in sectors or sub-sectors in 2022.

3.11.1.2 Activities

In cooperation with other central authorities, the Ministry of Economy of the Slovak Republic commented on the Strategy of Cyber Defence of the Slovak Republic and the Decree of the NSA, which determines knowledge standards in the field of cyber security.

The representative of the Ministry of Economy participated in several working groups related to cyber security. No activities beyond §9(1)(c) of Act No. 69/2018 on cyber security were carried out.

3.11.1.3 Planned activities

For full coordination in the field of cybersecurity in the sectors and subsectors for which it is responsible under the law, the MoE SR plans to create a post for coordination of cybersecurity in sectors and subsectors, respectively for communication and coordination of cybersecurity with the OESs.

3.11.2 Results of the audits of the Industry sector

In the Industry sector, only two audit reports have been submitted, so it is not possible to produce a sufficiently anonymised assessment of the results of audits in the sector.

3.12 Water and air

Central authority: the Ministry of the Environment of the Slovak Republic (MoEW SR)

Number of OESs: 20

Number of OESs with audit obligation in 2022: 20
(can also be fulfilled by self-assessment according to §34a (2) of Cyber Security Act)

Number of audit reports submitted: 11

Number of self-assessments submitted: 3

Subsectors: meteorological service, water construction, drinking water supply

3.12.1 ASSESSMENT OF THE STATE OF CYBERSECURITY FOR 2022 BY THE CENTRAL AUTHORITY

3.12.1.1 Threats

The most serious threats perceived by the MoEW are an unprecedented attack on an independent, directly neighbouring country, disinformation, the growing trend of phishing campaigns, distributed denial-of-service attacks and the energy crisis.

3.12.1.2 Activities

The MoEW focused its activities mainly on the Ministry itself. It submitted an application for a non-repayable financial contribution with a focus on the development of governance and the level of information and cybersecurity in the Water service sub-sector with the specific objective of increasing cybersecurity in society, priority axis No. 7 Information Society.

The ministry carried out training to raise the level of security awareness. It also communicated interest in collaborating in the implementation of the Investment No. 6 – Strengthening Prevention measures, Detection and Resolution of Incidents (ITVS), Component No. 17, as a part of Recovery and Resilience Plan project aimed at strengthening cyber security.

3.12.1.3 Planned activities

In the future, the MoEW intends to initiate a Memorandum of Cooperation for the implementation of the Investment No. 6 Strengthening Preventive Measures, Increasing the Speed of Detection and Resolution of Incidents (ITVS), Component No. 17, as a part of Recovery and Resilience Plan for Strengthening Cybersecurity, which was presented by representatives of the Cybersecurity unit of Ministry of Investments. Further, it intends to deepen cooperation with CSCCC, SK-CERT and the government's cyber incident response unit in the Slovak Republic, CSIRT.SK.

3.12.2 RESULTS OF OESS AUDITS IN THE WATER AND AIR SECTOR

The National Security Authority has received a total of 11 audit reports from the Water and Air sector as of December 31, 2022. Not all operators must carry out an audit, because in cases under the law some of them can choose to deliver self-assessments, which are not included in this statistic Based on the audit compliance statistics, in the Water and air sector, the average compliance percentage is as follows:

Average percentage compliance rate (year 2022)

COMPLIANCE	56 %
PARTIAL COMPLIANCE	15 %
NON-COMPLIANCE	23 %
NOT APPLICABLE	3 %
VERIFIED ELSEWHERE	2 %

source: 2022 audits, NSA

Looking at individual OESs in the Water and Air sector, compliance with audit requirements is more than half in the majority of operators. The highest compliance rate was achieved by the OES which, out of 266 audit requirements, achieved compliance in 200 requirements, partial compliance in 16 requirements and non-compliance in 19 requirements (16 requirements were not applicable and 15 were verified elsewhere).

On the other hand, the lowest level of compliance was identified for the OES which, out of 171 audit requirements, achieved compliance in 63 requirements, partial compliance in 58 requirements and non-compliance in 46 requirements (4 requirements were not applicable).

3.12.3 MOST FREQUENT AUDIT FINDINGS

The most common audit findings in the Water and Air sector include:

- in many cases, the content of the safety documentation is not fully implemented or does not reflect the actual status of the activities carried out,
- the principles of least privilege and distinction of competences are not implemented,
- the rules described in the policies are not put into practice,
- no central tool is implemented to monitor network events and no operational logs are recorded,
- there is no communication plan in place for the implementation of emergency plans and both emergency and recovery plans are not tested.

3.13 Public administration

Central Authority:
Ministry of Investment, Regional Development and Informatization of the Slovak Republic (MIRDI SR)
Ministry of Defence of the Slovak Republic (MoD SR)
Ministry of the Interior of the Slovak Republic (MoI SR)
National Security Authority (NSA)

Number of OESs: 1417

Number of OESs with audit obligation in 2022: 1416 (can also be fulfilled by self-assessment according to §34a (2) of Cyber Security Act)

Number of audit reports submitted: 99

Number of self-assessments submitted: 405

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

3. 13. 1 ASSESSMENT OF THE STATE OF CYBERSECURITY FOR 2022 BY THE CENTRAL AUTHORITY

3.13.1.1 Ministry of Defence of the Slovak Republic – Defence

3.13.1.1.1 Threats

In the assessed period, a number of cyber security incidents happened in the information and communication infrastructure of the Ministry of Defence of the Slovak Republic, the Armed Forces of the Slovak Republic and the institutions and organisations establishes under their jurisdiction.

In general, it can be stated that these were standard cyber security incidents, which do not stand out in their scope and character from the series of recorded cyber campaigns against NATO and EU member states in the context of the current geopolitical situation.

We consider the most serious cyber security incidents recorded in 2022 to be attempts to penetrate the information and communication infrastructure of the Ministry of Defence, as well as cyber security incidents caused by the so-called "insider threat". We consider DDoS attacks against the information and communications infrastructures we monitor to be significant from a geopolitical perspective, but with a lesser impact on department´s cyber security itself.

Compared to the past, last year saw a significant increase in the number and sophistication of phishing and scam campaigns. In this regard, more than 1,000 emails were investigated during the evaluation period.

3.13.1.1.2 Activities

In the field of cyber security, the Ministry of Defence cooperates with other central authorities and operators of essential services in fulfilling the tasks arising from Act No. 69/2018 on cyber security. In this context, the Ministry of Defence has concluded cooperation agreements in the field of cyber security and cyber defence with a number of national and international institutions, to which it provides various forms of services.

In general, this includes, but is not limited to, monitoring information and communication infrastructure, assisting and handling cyber security incidents, sending security alerts, conducting and providing training and education, and participating in cyber defence exercises.

A special task in the evaluated period was participation in conducting the cyber security audit in the conditions of the Air Forces of the Armed Forces of the Slovak Republic and the Central Military Hospital in Ružomberok – University Hospital.

In connection with the change in the security environment due to the outbreak of the armed conflict in Ukraine, the Ministry of Defence performed extraordinary tasks in the field of cyber security set by the Security Council of the Slovak Republic. These tasks were performed in close cooperation with the National Security Authority and the Slovak Information Service.

3.13.1.1.3 Planned activities

In addition to the normal activities resulting from national legislation, the main activity of the Ministry of Defence in the field of cyber security will be the implementation of the tasks set out in the Action Plan for the Implementation of the Cyber Defence of the Slovak Republic. The aim will be to strengthen and streamline the overall processes of cyber security management and performance in the conditions of the Ministry of Defence.

3.13.1.2 Ministry of the Interior of the Slovak Republic – security

3.13.1.2.1 Threats

The Ministry of the Interior of the Slovak Republic registered in the subsector of Security increased activities, threats and dangerous activities in the field of cyber security aimed at the infrastructure and information systems of the Ministry. After the outbreak of the conflict in Ukraine and especially after the political condemnation of this aggression and the ensuing restrictions against Russia, there was an increased number of offers for conducting cyber attacks on government institutions of the Slovak Republic, including the Ministry, critical infrastructure and strategic enterprises.

In addition, there was notable increase in attacks on infrastructure, particularly phishing and DDoS attacks, which, however, cannot be clearly linked to the conflict in Ukraine, but rather to developments in the region. The increasing number of phishing attacks against Ministry staff, the level and sophistication of which is on the rise, cannot be overlooked.

3.13.1.2.2 Activities

The Ministry of the Interior of the Slovak Republic has increased monitoring of cyberspace in the Ministry, including illegal websites, social networks, and communication platforms, where it has focused on the activities of hacker groups. Preventive activities were reflected by publishing actual security warnings, vulnerabilities and bulletins and their deployment and removal in the monitored infrastructure.

During the year, the Ministry focused on raising the cyber awareness of the its employees through cyber exercises, educational activities and expanding communication channels for reporting cyber incidents. It established a telephone support line for Department employees to address and report cybersecurity incidents, which is available nonstop. The Department has started the second phase of building technical capabilities focused on the Security Operations Center (SOC) dealing with security incident response, monitoring and oversight of the Department's infrastructure and information systems. They have also established cooperation with other central authorities and built up mutual communication channels for the immediate exchange of information.

3.13.1.2.3 Planned activities

The MoI SR as a central authority plans to complete the technical capabilities focused on the SOC unit in 2023 with the gradual implementation of the SIEM logging and monitoring system in order to identify and handle cybersecurity incidents.

As an important aspect of cyber security, the ministry also considers training of security administrators and raising security awareness and knowledge of the ministry's employees on a regular basis. Last but not least, we also plan to implement tools to protect data, data transmissions and communications against external threats and their potential misuse.

3.13.1.3 Ministry of Investment, Regional Development and Informatization of the Slovak Republic - Public Administration

3.13.1.3.1 Threats

Several types of threats were identified by the government's CSIRT unit last year. A particular significant factor was the outbreak of the military conflict in Ukraine and the related cyber-attacks by various groups, which also targeted public administration entities.

The unit saw a slight increase in reported cyber security incidents, up approximately 20% compared to the previous year. There has been a significant increase in the number of system intrusions (in0020total of 56) compared to the long-term average (2014 to 2021).

The number of recorded cybersecurity incidents caused by malicious code has also more than doubled compared to the long-term average. The main drivers of incidents are long-standing weaknesses identified in the subsector of Public administration – poorly implemented processes for early detection of vulnerabilities and deployment of patching updates; inadequate or completely absent security monitoring; neglected education and training of staff and the associated increased dangers caused by attacks using social engineering methods.

In addition, campaigns targeting the Slovak Republic's cyberspace were monitored, as well as global campaigns translated into Slovak language.

3.13.1.3.2 Activities

The Ministry, in cooperation with National Agency for Network and Electronic Services (NANES), has established a central security monitoring of the Government's Govnet (NANES), the public administration entities and the handling of cyber security incidents.

In addition, specialised laboratories were equipped for penetration testing, forensics and malware analysis. In order to detect vulnerabilities, IP addresses accessible from the Internet were regularly scanned by system Achilles during the year. A total of 165 organisations which participated in the vulnerability assessment service were scanned per month.

MIRDI SR updated and improved the published methodological guidelines and models of security documentation for public administration entities that implement minimum security measures in accordance with the requirements of Act No. 69/2018 on Cyber Security, Act No. 95/2019 on Information Technology in Public Administration and their implementing regulations.

In addition to the implementation of the tasks from the Government resolutions, it successfully concluded the program Development of Governance of Information and Cyber Security in the subsector of Public Administration and in healthcare institutions, which aimed to support the OESs and the authorities to increase the level of compliance with the legislative requirements imposed on them, in particular the inventory of assets, the processing of security documentation, risk analysis, the implementation of a log management system and a security operations centre as a service.

Almost half of the more than 120 applicants for non-repayable financial contributions for a total of EUR 20 million were towns and municipalities. MIRDI SR distributed information for cities and municipalities on methodological materials supporting the creation of security documentation, including the risk analysis methodology issued by the NSA.

At the same time, during 2022 the Government's CSIRT unit trained more than 500 employees of public administrations in regards to cyber security.

MIRDI SR will also create a central portal for cyber security and prepare a unified methodological framework, which will include the completion and updating of model documentation for OESs; the working group on legislation will focus on the possibilities of simplifying legislative requirements in the field of cyber security and information security.

3.13.2 RESULTS OF AUDITS OF THE OESS IN THE PUBLIC ADMINISTRATION SECTOR

As of 31.12.2022, the National Security Authority has received a total of 99 audit reports from the Public Administration sector. Not all operators must carry out an audit, because in cases under the law some of them can choose to deliver self-assessments, which are not included in this statistic Based on the audit compliance statistics, in the Public Administration sector, the average compliance percentage is as follows:

Average percentage compliance rate (year 2022)

SÚLAD	37 %
ČIASTOČNÝ SÚLAD	17 %
NESÚLAD	36 %
NEAPLIKOVATEĽNÉ	5 %
OVERENÉ NA INOM MIESTE	4 %

zdroj: Doručené audity 2022, NBÚ

The Public Administration sector has the lowest average compliance rate (and conversely the highest average non-compliance rate of all sectors – with the exception of the Thermal Energy subsector, however, there are significantly fewer OESs).

The highest level of compliance was achieved by the OES, which was compliant in 230 out of 233 audit requirements, partially compliant in 2 requirements and had no non-compliance in any of the requirements (1 requirement was not applicable).

On the other hand, the lowest level of compliance was identified for the OESs which, out of 179 audit requirements, achieved compliance in 5 requirements, partial compliance in 61 requirements and non-compliance in 109 requirements (4 requirements were not applicable).

3.13.3 MOST FREQUENT AUDIT FINDINGS

The most frequent audit findings in the Public Administration sector include:

- ystem of cybersecurity management has not been prepared,
- No cyber security strategy or other security documentation has been submitted,
- The cybersecurity manager is not formally appointed, has conflicts of interest and inappropriately cumulative responsibilities,
- risk analysis is not established as a process in internal rules or methodologically described and it is not carried out,
- there are highly privileged accounts in the organisation that are shared among more people and do not have defined owners and their purpose,
- the organisation does not have a definition of a major cyber security incident, has not developed procedures and does not have sufficient capabilities to detect, manage and learn from potential incidents.

3.14 Healthcare

Central authority: the Ministry of Health of the Slovak Republic (MoH SR)

Number of OESs: 90

Number of OESs with audit obligation in 2022: 85
(can also be fulfilled by self-assessment according to §34a (2) of Cyber Security Act)

Number of audit reports submitted: 61

Number of self-assessments submitted: 13

Subsectors: Health facilities (including hospitals and private clinics)

3.14.1 Assessment of the state of cybersecurity for 2022 by the central authority

3.14.1.1 Threats

Due to the sensitivity of healthcare data, the healthcare sector is increasingly exposed to cyber threats and incidents threatening the security of data, availability and quality of healthcare. Healthcare facilities have outdated information and communication technologies and their staff does not have insufficient cyber security awareness.

The most serious threats in the healthcare sector are the lack of support from the top management of the organisation and the related lack of adequately allocated funds which are needed to increase and develop the sufficient level of cyber security; the lack of complexity of IT systems due to the use of a number of different tools and solutions; inappropriately shared responsibility for security in the use of cloud-based solutions; vendor lock-in and IoT devices containing numerous and easily exploitable vulnerabilities.

However, by building resilience to cyber threats through good security measures and other best practices, or by improving incident detection and response, the sector can be protected.

3.14.1.2 Activities

The Central Authority for the Health Sector, within the meaning of the provisions of Article 9(1) (c) of Act No. 69/2018 on Cyber Security, actively cooperates with the units that, within their competence, are responsible for dealing with cyber security incidents and carry out preventive services and reactive activities.

The Ministry of Health of the Slovak Republic guides organisations under its founding, establishment and shareholder competence in the field of cyber security.

The Security Committee of the Ministry of Health of the Slovak Republic for the area of information and cyber security, as an advisory body to the Minister, discussed and decided on issues aimed at eliminating and solving the consequences caused by cyber incidents in the health sector.

In order to respond to cyber attacks in a timely and effective manner, there is a project ongoing which aims to implement a central tool for monitoring the activities of networks and information systems and their users, providing security oversight of networks and information systems by monitoring the traffic in these networks and information systems.

In terms of the project Development of Governance and Information and Cyber Security in the subsector of the Public Administration, there is an ongoing contract for the providing of a non-repayable financial contribution to increase cyber security in the health sector.

3.14.1.3 Planned activities

In order to reduce the extent of damage caused by the exploitation of a specific vulnerability by a specific threat, the central authority for the health sector shall develop security incident response procedures for the most frequently occurring security threats arising in the field of health care.

In connection with the transposition of Directive (EU) 2022/2555 of the European Parliament and of the Council on measures to ensure a high common level of cybersecurity in the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS 2 Directive), the Ministry of Health will start communication with the National Security Authority in defining the types of entities in the health sector in the context of the preparation of the amendment to Act No 69/2018 on cybersecurity.

3.14.2 RESULTS OF AUDITS OF OESS IN THE HEALTH SECTOR

The NSA has received a total of 61 audit reports from the Health sector as of 31 December 2022. Not all operators must carry out an audit, because in cases under the law some of them can choose to deliver self-assessments, which are not included in this statistic Based on the audit compliance statistics, in the Healthcare sector, the average compliance percentage is as follows:

Average percentage compliance rate (year 2022)

COMPLIANCE	42 %
PARTIAL COMPLIANCE	15 %
NON-COMPLIANCE	35 %
NOT APPLICABLE	4 %
VERIFIED ELSEWHERE	4 %

source: 2022 audits, NSA

In the Healthcare sector, there is less than half the compliance rate with audit requirements across all operators, along with a high level of non-compliance.

The highest compliance rate was achieved by the OES, which achieved compliance in 202 out of 266 audit requirements, partial compliance in 16 requirements and non-compliance in 21 requirements (13 requirements were not applicable and 14 were verified elsewhere).

On the other hand, the lowest compliance rate was identified for the OES which, out of 266 requirements audited, achieved compliance in 6 requirements, partial compliance in 23 requirements and non-compliance in 210 requirements (15 requirements were not applicable and 12 were verified elsewhere).

3.14.3 MOST FREQUENT AUDIT FINDINGS

The most common audit findings in the Health sector include:

- the cyber security governance, execution of processes and control structure is not defined for the OESs,
- Rules and responsibilities for implementing the measures resulting from the risk analysis are not established, as well as responsibility for identifying and registering assets
- OESs does not adequately take care of encryption protection of information,
- Most encryption and key management processes are not formalised,
- remote access to internal networks and IS is not secured.

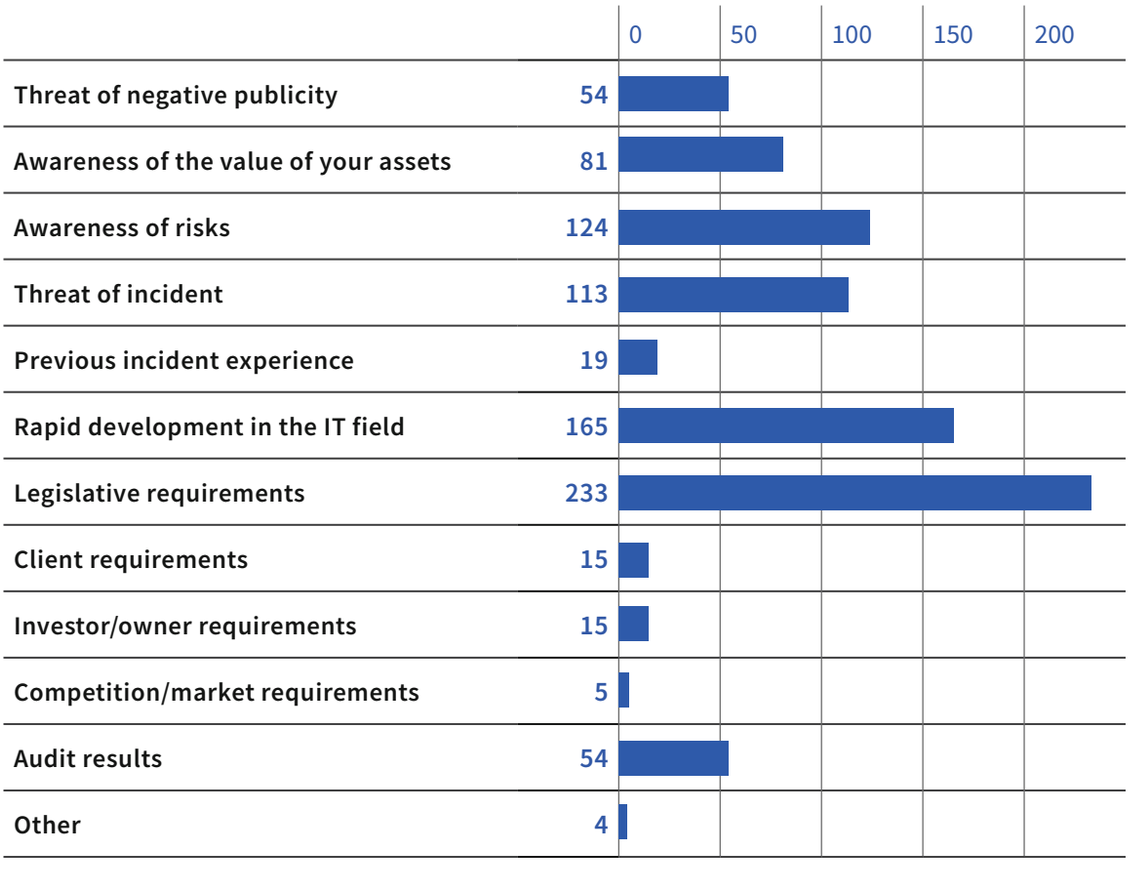
3.15 Survey on the state of cyber security in the OESs

The National Cyber Security Centre SK-CERT conducted a survey among OESs on the state of cyber security in 2022. The survey was conducted on a voluntary basis, with data provided by a total of 270 operators across sectors. The questions in the survey aim to evaluate multiple aspects of management, funding and development of cyber security in regulated entities.

3.15.1 FACTORS INFLUENCING THE IMPROVEMENT OF CYBER SECURITY

From the perspective of OESs, without distinction of sector, among the factors influencing the improvement of the level of cybersecurity in the organisation, the leading factors are legislative requirements, followed by rapid development in the IT field and awareness of risks (OESs could choose multiple options).

What are the most influencing factors in your organization in increasing the level of cyber security?



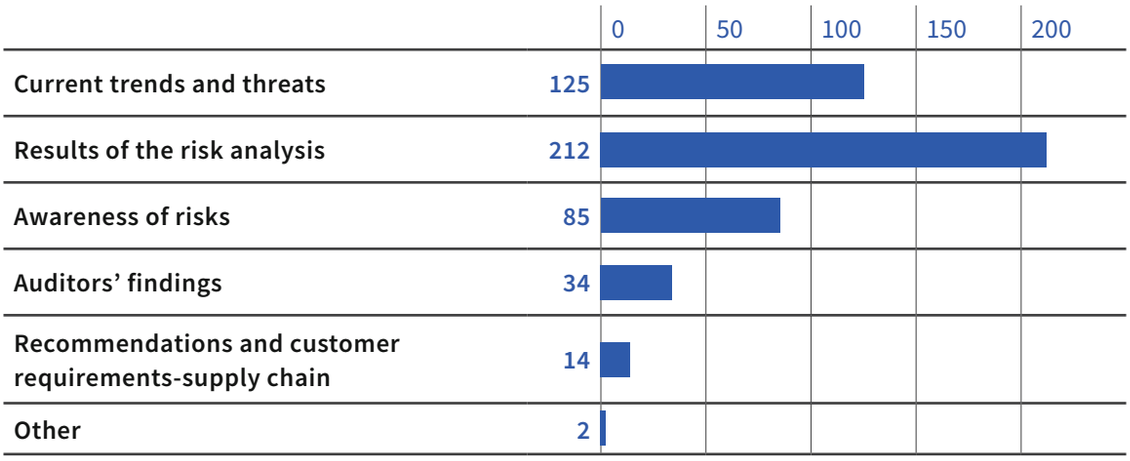
Source: survey among OESs, NCKB SK-CERT, March 2022

If we look at the question from a sectoral perspective, we find a slightly different view in the Transport sector, where the most significant factor in increasing the level of cyber security is the result of an audit, in the Electronic Communications and Digital Infrastructure sectors it is the threat of an incident, in the Energy sector it is the awareness of the value of its own assets, and in the Healthcare sector the most significant factor is the awareness of the risks and the threat of an incident occurring.

3. 15. 2 IDENTIFYING PRIORITIES AND DIRECTIONS IN CYBER SECURITY

According to survey, OESs define their priorities and progress in the area of cyber security based mainly on risk analysis, current trends and threats, and audit results.

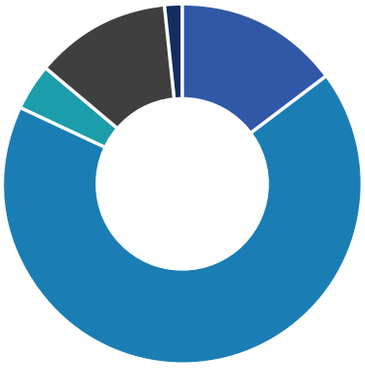
What are the factors that have the most influence in your organization to improve the level of cybersecurity?



Source: survey among OESs, NCKB SK-CERT, March 2022

3. 15. 3 PERCEPTION OF THE ACTIVITIES OF THE CENTRAL AUTHORITY

The activities of the various central authorities (the body responsible for the sector under the Cybersecurity Act) are perceived by most of the OESs to be from very good to satisfactory. However, up to 12.2% of operators do not perceive any activities or actions of the Central Authority (especially in the Public Administration sector).



How do you perceive the activities and operation of the central authority under Cyber security Act 69/2018, which is responsible for your sector?

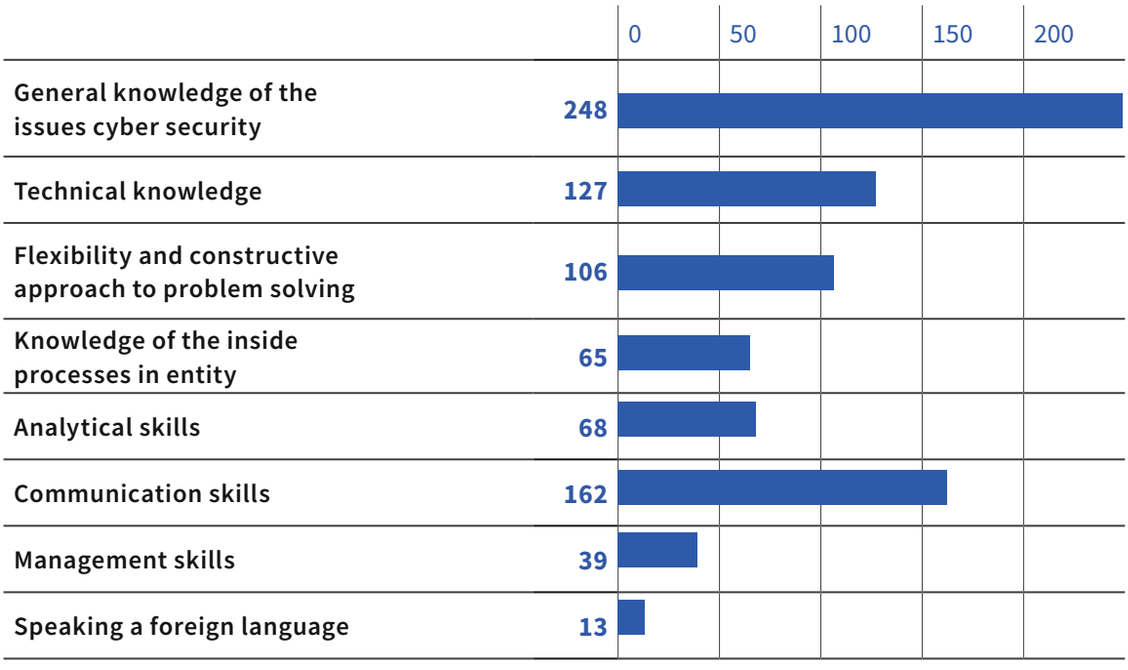
VERY GOOD	14,8 %
SATISFACTORY	67,4 %
I AM NOT AT ALL SATISFIED WITH THE ACTIVITIES AND THE ACTION OF THE CENTRAL AUTHORITY	4,1 %
I DO NOT PERCEIVE ANY ACTIVITY, OR THE OPERATION OF THE CENTRAL BODY	12,2 %
OTHER	1,5 %

Source: survey among OESs, NCKB SK-CERT, March 2022

3. 15. 4 EXPERIENCE AND KNOWLEDGE OF OES´S CYBER SECURITY EMPLOYEES

Most OESs value general knowledge of cybersecurity issues, communication skills and technical knowledge among its staff. Slightly more different is the Digital Infrastructure sector, where analytical skills are most valued, and the Water and air sector, where operators most value flexibility and a constructive approach to problem solving (OESs could choose multiple options).

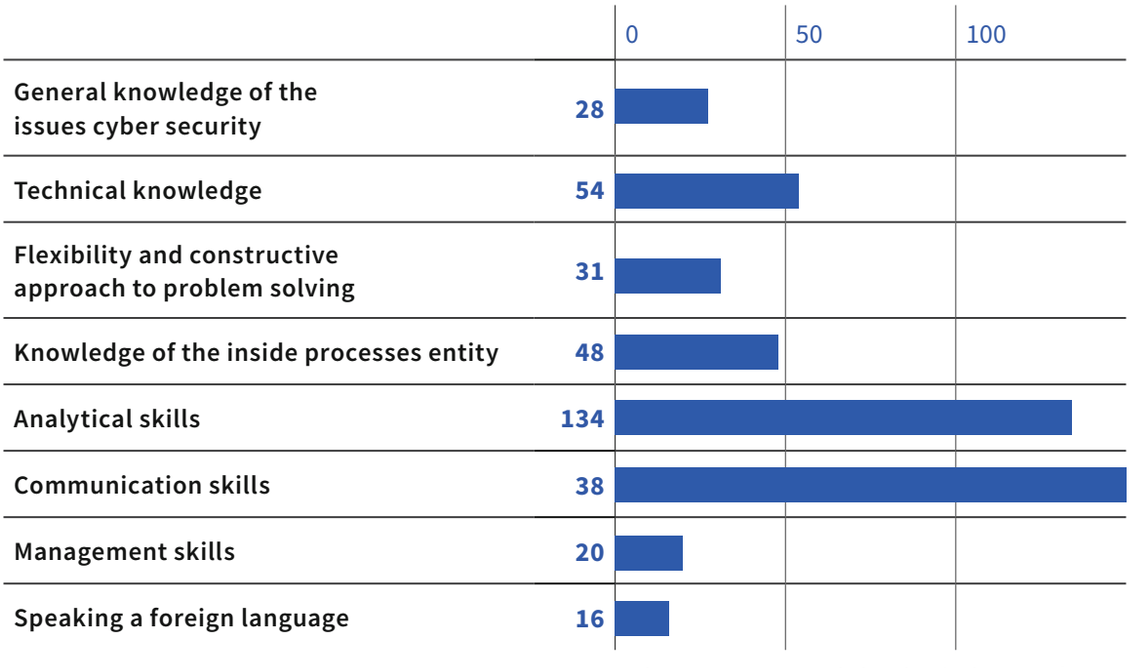
Which knowledge and experience of cybersecurity personnel do you value the most?



zdroj: Prieskum názorov PZS za rok 2022, NCKB SK-CERT, marec 2022

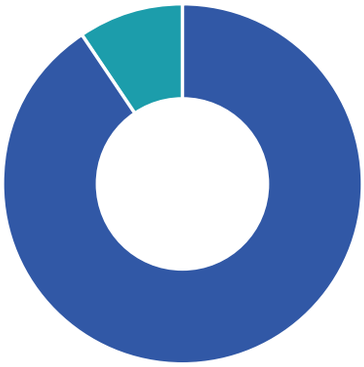
According to operators, the most missing knowledge and skills are analytical skills, technical knowledge and knowledge of the inside processes in entity (OESs could choose multiple options).

Which skills and experience of cyber security personnel do you consider to be most lacking at the moment?



Source: survey among OESs, NCKB SK-CERT, March 2022

Most of the OESs provide cybersecurity awareness training opportunities for their employees, and most of them also make such training mandatory.



Do you provide your employees with awareness-raising opportunities in cybersecurity?

YES	**90,7 %**
NO	**9,3 %**

zdroj: Prieskum názorov PZS za rok 2022, NCKB SK-CERT, marec 2022

Is such training for your employees compulsory or voluntary?

COMPLIANCE	**73,3 %**
PARTIAL COMPLIANCE	**17,4 %**
NON-COMPLIANCE	**9,3 %**

Source: survey among OESs, NCKB SK-CERT, March 2022

3. 15. 5 CYBER SECURITY MANAGEMENT

The implementation of security measures beyond the law is carried out by 25 % of the surveyed operators and these are mostly operators in the Banking sector (regulation in the financial sector) and in the Public Administration sector (Act No. 95/2019 on Information Technology in Public Administration).

A number of operators have indicated that they are implementing measures under Law No 18/2018 on the protection of personal data (or under the GDPR). When asked about this, some controllers responded that they follow international standards (which are not legally binding).

Do you implement security measures above and beyond the law?

YES	**25 %**
NO	**75 %**

Source: survey among OESs, NCKB SK-CERT, March 2022

The majority of operators carry out regular assessments of the security on their own initiative.

Do you in carry out regular assessments the effectiveness of adopted security measures on your own initiative?

YES	**74,4 %**
NO	**25,6 %**

Source: survey among OESs, NCKB SK-CERT, March 2022

Almost 62% of OESs have developed business continuity management (BCM) for their organisation, but only 12% of them carry out a regular test and validate its effectiveness at least once a year.

The most significant difference between the existence of BCM and their regular testing is in the Public Administration sector, where only 8.6% of the entities that have BCM in place also regularly test them. In contrast, in the Digital Infrastructure sector, almost 67% of the surveyed entities test their plans regularly.

Did you prepared plans of Business Continuity Management?

YES	**38,2 %**
NO	**61,8 %**

Source: survey among OESs, NCKB SK-CERT, March 2022

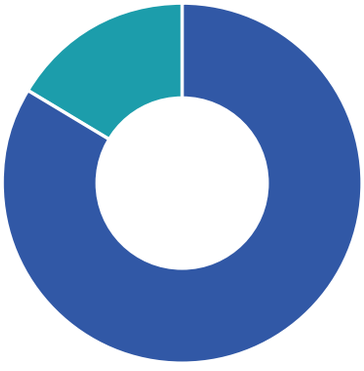
Do you perform a test of BCM plans to verify its usability, at least once a year?

YES	**12,6 %**
NO	**87,4 %**

Source: survey among OESs, NCKB SK-CERT, March 2022

3.15.6 FUNDING

The cybersecurity budget is part of the IT budget in more than 83% of surveyed operators. The cybersecurity budget for most operators is flexible, i.e. it changes as needed.



Is a budget for cyber security part of the IT budget?

YES	**83,7 %**
NO	**16,3 %**

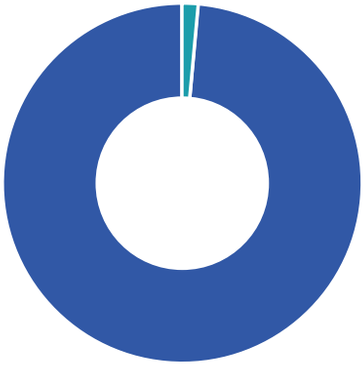
zdroj: Prieskum názorov PZS za rok 2022, NCKB SK-CERT, marec 2022

How do you set your annual budget on cyber security?

IT'S FIXED	**12,6 %**
VARIES AS REQUIRED	**87,4 %**

Source: survey among OESs, NCKB SK-CERT, March 2022

OESs do not typically set aside specific funds for emergencies – only 1.5% of respondents have funds set aside to cover BCM.

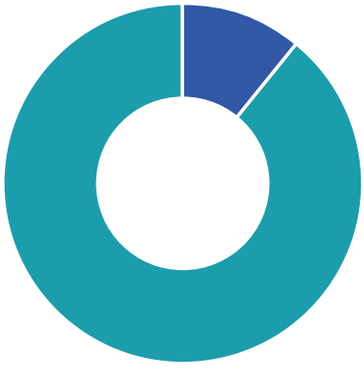


Do you have a separate budget for BCM (e.g. exceptional situations)?

YES	**1,5 %**
NO	**98,5 %**

Source: survey among OESs, NCKB SK-CERT, March 2022

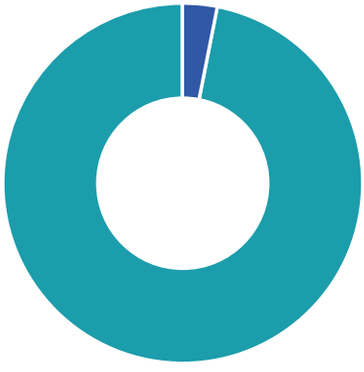
Respondents usually do not have an insurance, either for their assets or in relation to cyber security (which may be also caused by insufficient market offer of this type of insurance).



Do you have insurance for your information assets?

YES	**11,1 %**
NO	**88,9 %**

zdroj: Prieskum názorov PZS za rok 2022, NCKB SK-CERT, marec 2022



Do you have insurance in relation to to cybersecurity?

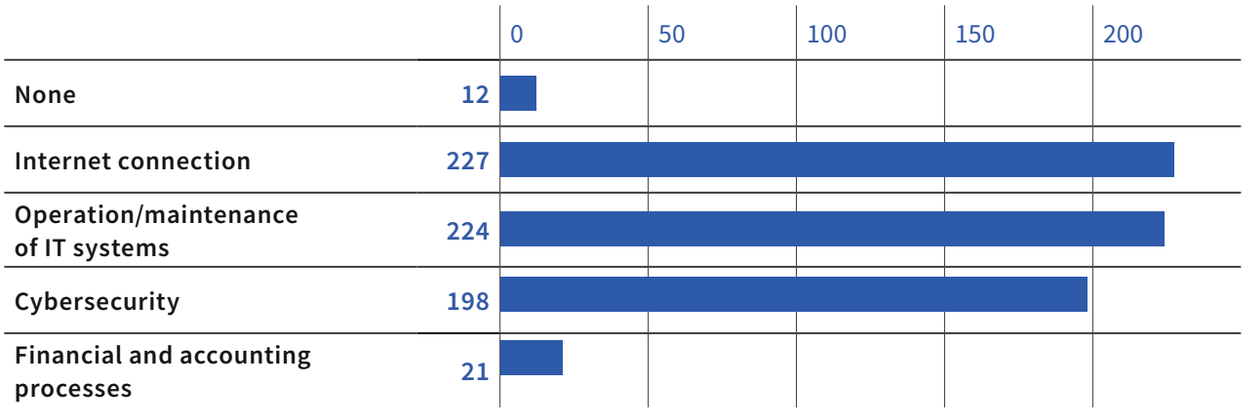
YES	**3,3 %**
NO	**96,7 %**

Source: survey among OESs, NCKB SK-CERT, March 2022

4. 15. 7 OUTSOURCING

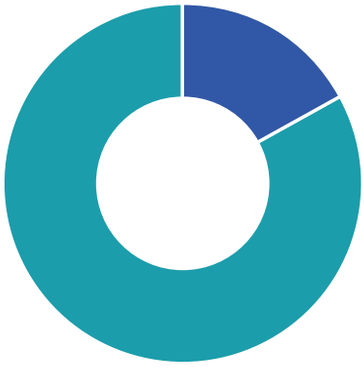
The most frequently used external IT services by the respondents are internet connectivity, operation/maintenance of IT systems and maintaining cyber security.

In which areas do you use external resources/processes (outsourcing)?



Source: survey among OESs, NCKB SK-CERT, March 2022

Managed Security Services (MSS) are used by 17% of the surveyed operators, with the majority of operators using cyber security services.



For cyber security, do you use services of MSS providers, which offer some areas of cyber security as a service?

YES	**17 %**
NO	**83 %**

Source: survey among OESs, NCKB SK-CERT, March 2022

4 CYBER SECURITY EDUCATION

4.1 Education in primary and secondary schools

Compared to 2021, there was no change in primary and secondary education. This is underlined by the state of implementation of the tasks in the field of education resulting from the Action Plan for the Implementation of the National Cyber Security Strategy 2021-2025. Once again, we have to acknowledge that education and the cyber security awareness is not formally addressed in primary schools at all.

Education in this field should be subject to the latest technological trends and knowledge. In the syllabus of the Ministry of Education, Science, Research and Sport of the Slovak Republic, cyber security is taught only very marginally in computer science classes.

If we consider how broad the issue of cyber security is and compare it with the actual hourly allocation of computer science in individual schools, where pupils are supposed to learn not only cyber security, but especially digital literacy, we can conclude that current level of education is absolutely insufficient.

Cybersecurity is a cross-cutting topic and therefore one would expect to see teaching in this area in subjects other than computer science, but this is also not happening. This minimalistic approach to teaching at least the basics of cybersecurity only make the problems worse, which in turn leads to higher rates of cyber attack victims, but also to a lack of experts in the field of cyber security.

Thus, the absolute lack of interest in cyber security issues in education by the competent authorities must be replaced only by enthusiastic teachers, civic associations and a few individuals. However, they cannot sufficiently replace all that is needed.

The lack of teaching supplements, which are also created only thanks to the enthusiasm of individuals and non-government associations, the lack of time allocation, as well as the lack of teachers in the field of cyber security, will inevitably lead to stagnation over the years and only worsen the problems that may cause an irreparable deficit in cyber security awareness.

4.2 Universities

In 2021, the NSA and CSCCC carried out a survey relevant at universities, that reflected the state higher education in the field of cyber security security in Slovakia.

The survey was mainly aimed at identifying the current status of the existence of accredited study programs, departments or subjects. For the year 2022, it can be stated that the situation in this area has not changed and the relevant universities that indicated the existence of a program, department or subject have retained their accreditation.

Accreditation of the program, department or subject is the long-term process and final results of the efforts of other universities, which started with efforts for accreditation recently will be visible in the years to come.

However, it can be stated that the education of experts is making better progress at universities than the general cyber security education at the lower levels of education. Relevant universities had realized the importance of training professionals. They can however, run into several problems, for example, students' lack of interest in studying cyber security, as they prefer other fields of study.

Despite the continuous improvement in the level of education of cyber security at universities, these efforts still cannot cover the sufficient number of graduates which of is needed by labor market.

4.3 Education of adults

The education of adults in cyber security is also a responsibility of the CSCCC as a contribution organization of the NSA. Adult education is one of the options how to start fulfilling the needs of the labor market in cyber security.

In 2022, the key issue was the preparation of a new set of specialization courses and workshops for current as well future cyber security managers.

During the monitored period, CSCCC succeeded especially in:

- issued an updated Cyber Security Education Scheme
- updated several existing cyber security courses included a new type of practical educational activity – workshop – in the training portfolio
- opened new trainings (both for public and non-public):
  - risk management in cyber security (1 day course + 1 day workshop)
  - classification of information and categorization of networks and IS (1 day course + 1 day workshop)
  - information security management according to ISO/IEC 27001
- implemented activities in the framework of increasing security awareness:
  - participation in professional cyber security conferences (EPI, ITAPA)
  - participation in communication activities for the professional and general public on the CSCCC website and social networks

In 2022, CSCCC also conducted a total of **5** "Cyber security Overview" **courses**, 20 "Cyber security Manager" courses and **12 specialization courses** and workshops. A total of **473 participants** took part in these activities.

The CSCCC sees room for further improvements in 2023, in particular again in reaching an agreement on co operation in education with other public administration entities, namely MIDRI and local government bodies.

5 EVALUATION OF THE IMPLEMENTATION OF THE ACTION PLAN OF THE NATIONAL CYBER SECURITY STRATEGY FOR THE YEARS 2021 TO 2025

For the purpose of evaluating the Action Plan for the implementation of the National Cyber Security Strategy for 2021-2025, the NSA established a Monitoring Committee for the implementation of the Action Plan.

This Committee shall be an independent advisory body to the Director of the Authority. Its duty is to monitor and coordinate the implementation of the tasks arising from the Action Plan. The Committee shall be chaired by an officer of the Authority and its members shall be representatives of all the entities that have at least one task in the Action Plan.

One of the tasks of the Monitoring Committee is to prepare an annual report on the implementation of the tasks of the Action Plan. It is always evaluating the previous year. The evaluation of 2022 also includes of the tasks that have not yet been completed in 2021.

The status of individual tasks can be set as:

- **fulfilled** – the task is completed in accordance with the measurable indicators,
- **Ongoing** – tasks with a time horizon of 'ongoing', and such tasks are indicating how they will be completed on an ongoing basis,
- **in progress** – the entity has not yet completed the task, but indicates that it is working on it and plans to complete it,
- **unfulfilled** – the entity has not completed the task and has not indicated whether it is working on it or plans to complete it,
- **unknown** – the responsible entity has not sent a deduction for the task.

Implementation of the tasks in the Action Plan is progressing only in some areas. Many multiobjective tasks are in a state of work in progress. The worst area of task implementation is education. The entity with the most tasks in this area, the Ministry of Education, Science, Research and Sport, has indicated almost all tasks as unfulfilled, without any indication of where the individual tasks really stand.

This is one of the most important areas in the field of cyber security and the responsible entity does not give it adequate importance and by delaying individual tasks it is moving away from meeting the strategic objectives identified in the National Strategy for Cybersecurity for 2021-2025.

An evaluation of the implementation of the Action Plan, together with a detailed description of the status of implementation of each task, is provided in the Annex to this report.

6 ACTIVITIES AND MEASURES

The NSA also in 2022 confirmed its orientation in building a security environment that corresponds to the principles adopted in the European Union Strategy for the Security Union for the period 2020-2025 and the EU Cyber Security Strategy for the Digital Decade.

Improving cyber infrastructure resilience, cyber security and setting up processes to ensure security in both physical and digital environments are still to be the main priorities.

In terms of the development of the NSA´s international relations, it continued to work within the framework of the international representation of the Slovak Republic, where it participated and contributed to the development of security policies at the EU and NATO, and also took part at various international activities, bilateral relations and regional cooperation.

6.1 National legislation

In 2022, the NSA responded to the growing number of actors in the disinformation scene in cyberspace with legislative changes to **Act No. 69/2018 on Cyber Security.**

The Act No. 55/2022 on certain measures taken in regard to the situation in Ukraine made the Authority obligated to make decisions on blocking harmful content or harmful activity directed to/from the cyberspace of the Slovak Republic and to ensure the actual implementation of the blocking (with a transitional limitation until 30 June 2022).

Act No. 231/2022, amending Act No. 69/2018, extended this deadline to 30.9.2022.

In May 2022, a draft law amending Act No. 69/2018 was submitted for interministerial comment procedure, the aim of which was to reflect some issues of application practice in relation to the execution of blocking, liability, procedural procedure for issuing a decision and its implementation, and the regulation of the publication of decisions on the Authority's website. In November 2022, the government bill was submitted to the National Council of the Slovak Republic (1st reading), but the bill did not pass to the next reading.

Furthermore, in 2022, the Authority implemented the legislative process of the two implementing regulations of **Law 69/2018. The original draft amendment to the National Security Authority's Decree No. 436/2019** on the Cyber security Audit and Knowledge Standard auditor was transformed during the legislative process into a draft of a new decree on cyber security audit in order to update the rules for conducting a cyber security audit, its duration, periodicity, and the requirements for the final report on the results of the audit. New decree of the National Security Authority

No. 493/2022 on cyber security auditing came into force on 1 January 2023. Decree of the National Security Authority No. 492/2022, which establishes knowledge standards in the field of cyber security, aims to define the minimum expertise for individual users of networks and information systems carrying out cyber security activities and tasks.

The knowledge standards also form a framework for the creation of educational programmes at educational institutions, thus filling the space not only for building quality security awareness in the field of cybersecurity, but also for improving the quality of educational processes. This in turn will also affect the quality of the personnel carrying out cyber security activities in public and private organisations. The introduction and definition of knowledge standards and their application in the field of cyber security is an essential element of building a stable and predictable security environment. This decree also entered into force on 1 January 2023.

6.2 European Union

Employees of the NSA participated in regular meetings of the Security Committee of the Council of the EU (CSC), the European Commission's Security Policy Expert Group (ComSEG) and the Security Committee of the European External Action Service (EEAS).

The review of the security rules continued in 2022 at the EU Council in order to address the shortcomings identified in application practice and to increase the comfort for the receivers of these rules. In the working formats mentioned above, the Authority was actively involved in the preparation of security standards in order to enhance the level of protection of classified information and continued to be actively involved in the process of revision of the security rules.

In the area of protection of classified information, the most discussed topic at the EU was the forthcoming EC Regulation on common uniform rules for the protection of EU classified information for all EU institutions, bodies and agencies. Member states agree that the (legal) basis for all EU security rules is laid down by the Council in the documents in force.

At the regular meeting of the Security Committee of the European External Action Service (SC EEAS), the EEAS reviewed their security awareness programme and stepped up staff training on potential cyber risks. In this context, they are preparing a handbook to help not only newcomers in working with EUCI. EEAS staff have contributed to building resilience and security awareness in EU Delegations abroad through training, workshops and outreach programmes.

The NSA was regularly and actively represented at the meetings of the Horizontal Working Party on Cyber Issues (HWPCI) during the French and Czech Presidencies of the Council of the EU.

Regarding legislative issues, 2022 was an important milestone for strengthening EU cybersecurity, with the adoption of a Directive setting out rules to ensure a high common level of Union cybersecurity (NIS Directive 2). Its transposition into national legislation will be a key task for the Authority.

Another important and follow-up step was the presentation of the draft legislation on cyber resilience, which sets out cyber security requirements for products with digital elements.

A crucial task in this regard will be to set clear rules to ensure a high level of EU cyber security, with a vision of setting standards for the rest of the world.

The HWPCI meetings also dealt with the negotiation of non-legislative documents. The most important of them, in the form of which the NSA also participated, were the Strategic Compass, the EU Council Conclusions on the cyber posture of the Union, the Council Conclusions on the security of the ICT supply chain, and the proposal for a new cyber defence policy presented in the EC's so-called defence package. The area of cyber diplomacy has been greatly influenced by situation on the EU's eastern border.

The HWPCI meetings were therefore also focused on the formulation of the texts of the EU High Representative's statements condemning the cyber-attacks on Ukraine by Russian actors that preceded and continued during Russia's invasion of Ukraine. In this context, the issue of revising the Cyber Diplomacy Toolkit (CDT) has been raised several times.

At the main Security Committee for EU Space Programmes at the European Union Space Programme Agency (EUSPA), the development of Programme Security Instructions (PSIs) was the main point of discussion.

Extensive documents have been prepared in the various supporting working groups, e.g. the Galileo Security Working Group, GOVSATCOM, Copernicus or Egnos. New EC initiatives have been set up in the context of the GOVSATCOM programme, such as the EuroQCI (Quantum Communication Infrastructure) ad hoc group, which contributes to the discussion on the cross-cutting theme of quantum communication infrastructure. It is to be used in the context of the GOVSATCOM programme and is intended to ensure a high level of encryption, resilience and ultimately security, as this network is also to be adapted for the transmission of classified information.

The key priorities of the Cooperation Group continue to be the implementation of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high level of network and information systems security in the European Union (NIS Directive) and the related application of the individual instruments.

In 2022, other important topics such as "Risk assessment and risk scenarios" have been added to this task which also follows from the task for the Cooperation Group and from the conclusions of Council for the development of an EU position on cyber security, "Crisis management", "Organisation and potential areas for future cooperation in the

Cooperation Group" and "Coordinated vulnerability disclosure".

ENISA conducted a roadmap of needs of cyber security exercise and countries shared their experiences on the most serious cyber security incidents and threats that affected them during the year (once again, ransomware dominated).

In 2022, the Authority and SK-CERT were active in several **Work Streams** of the Cooperation Group:

Work Stream 3 – Group focusing on notification obligations of OESs. As part of its work, the group worked on improving the various tools that serve the notification obligations for member countries. At the same time, the MSs worked on the preparation of an "Annual Report", which included direct input from MSs, thus fulfilling their information and notification obligations. The final report is always approved by the Cooperation Group and the Authority comments on it and sends its input.

Work Stream 7 – Cybersecurity Incidents of Large Scale Response Group. At the level of this group, the development of operational procedures for dealing with major incidents with an international dimension has continued and representatives of the Authority are actively participating in them.

Work Stream 10 – Digital Infrastructure Group. Within the platform, the 2022 MSs addressed the competent authorities and their obligation to define and follow a common approach to implementation requirements for digital service providers (DSPs). The intention of the NIS Directive was to define a maximum harmonisation framework for DSPs, which will be subject to the jurisdiction of a single competent authority (the competent authority in the country of head office in the EU) for all their activities in the Union.

Work Stream 5G – Group securing and protecting 5G networks. At the EC level, the Authority has been active in the Working Group on Cybersecurity in Fifth Generation (5G) Networks. The EC has published a set of recommended measures to mitigate the risks associated with the construction and operation of 5G networks, the so-called 5G Toolbox. The application of these measures has also been transferred to the national level, in particular in the form of application practices.

Work Stream 12 – Healthcare Sector Group – The experts working in this working group had to deal with the current challenges posed by the COVID-19 cyber security pandemic in the healthcare sector. At the same time, they are actively working on a draft document on the implementation of the NIS Directive (sectoral rules and recommendations regarding the setting up of cyber security measures in a given segment) in the healthcare sector, which is fast moving forward. Another objective of this platform is to increase the cyber security measures of entities that are part of the healthcare sector.

The new Work stream 15 – Supply Chain Security Group, where the Authority also confirmed its membership after it was formed, will focus during 2022 on strengthening ICT supply chain security and also on the first steps to address the threat of problematic strategic dependencies in ICT supply chains.

During the year, the **EU CyberNet** stakeholder community, which brings together national authorities and institutions working in the field of cyber security, expert groups in the field, think tanks and academic institutions based in EU Member States, also gained in importance. During the year, the EU CyberNet organised a number of workshops and conferences on current cyber security issues, with NSA´s employees were increasing their expertise and knowledge by actively participating in these activities and thus building the capacity of the Authority.

6.3 NATO

The operation environment of the North Atlantic Treaty Organisation (NATO) has been greatly influenced by geopolitical developments, in particular the situation in Ukraine – one of NATO's main partners with aspirations for accession.

The cyber-attacks on Ukraine carried out by Russian actors, which preceded the unprovoked invasion itself and are still ongoing, were in public statements unequivocally condemned by NATO Secretary General Jens Stoltenberg.

The Cyber Defence Committee (CDC) has been extensively engaged in providing assistance to the war-affected partner as well as expediting its entry into Cooperative Cyber Defence Centre of Excellence in Tallinn. The war in Ukraine has also provided some lessons from the uncoordinated approach to the provision of assistance and the Madrid Summit in July brought about an agreement by the Allies to establish a virtual cyber rapid response unit, which would voluntarily bring together cyber experts who would work together to respond to serious malicious cyber activity.

Last year there was the first meeting of national cyber coordinators at the North Atlantic Council (NAC). The main topic of discussion was national cyber defence contributions to the overall Alliance force for deterrence and defence in response to the events of the war in Ukraine. The Director of SK-CERT attended the meeting on behalf of the Slovak Republic.

NATO Security Committee (SC) meetings continued to take place in all their formats – in the format of Security Policies, Communications and Information Systems Security (CISS) and at the highest level – the level of the directors of the MSs security authorities. This year has been also an important in terms of protection

NATO classified information, marked by the continuation of a major review of NATO security rules.

The Authority also participated in the Capability Team meeting and presented its proposals for changes to the Classified Projects and Industrial Security Directive to the NATO Security Office (NOS) and delegates during the October meeting. The Communications and Information Systems Security format of the NATO SC addressed two main documents, the Cybersecurity Directive and the NATO Strategy on Artificial Intelligence (AI). During the October meeting at the highest format (Principals level), the 2023 agenda was presented to the participants and expanded with 2 new supporting documents.

The first will deal with remote work and the second addresses Foreign Ownership, Control and Influence (FOCI) on companies participating in NATO contracts.

6.4 Regional cooperation

Based on the rotation of the chairmanship of the countries that are members of the Central European Cybersecurity Platform (CECSP), the NSA, on behalf of the Slovak Republic, chaired this platform in 2022. The countries of the Visegrad Four (Czech Republic, Hungary, Poland, Slovak Republic) and Austria are represented in the platform with their experts. The Authority organised a high-level working personal meeting with the partners, which took place on 12 September in Bratislava.

The discussions focused on current issues that resonated at EU level throughout 2022, while at the same time the partners sought to find common ground and mutual support on these topics.

Among the most important topics were: “New challenges that require an adaptive, coordinated and innovative approach to the transposition of the NIS 2.0 Directive” and “Coordinated Vulnerability Reporting”.

The efforts of the Slovak Republic were also highlighted by a presentation dedicated to establishing a competence centre in the Slovak Republic’s cybersecurity regulatory system and we presented our concept for the cybersecurity community in the country. A complex and comprehensive study concerning the cybersecurity audit in Slovakia was presented by a representative of the CSCCC. Experts exchanged some knowledge and gave examples of good practice regarding the preparatory process of transposition of the NIS 2.0 Directive.

6.5 Bilateral relations

The Authority has developed bilateral relations on a daily basis across all working platforms, whether in contact during working group meetings or in the ad hoc execution of tasks specifically at the bilateral level.

The NSA signed an international bilateral agreement between the Government of the Slovak Republic and the Government of the United States of America on security measures for the protection of classified information. The new agreement significantly contributes to the deepening of relations and intensification of cooperation between both countries.

During the year, communication on the conclusion of a classified information protection treaty with the Kingdom of the Netherlands was launched, which is proving to be an important priority for the coming period in view of the application practice. Cooperation has also been expanded towards East Asia when two foreign visits from the Republic of Indonesia took place, during which the visitors were interested in the field of protection of classified information and cyber security.

Closer cooperation has been established in both issues with an expectation to conclude an international

treaty on the protection of classified information, as well as a memorandum of understanding on cooperation in the field of cyber security. In the context of international co-operation, a study work trip was carried out in September within the framework of the EU TAIEX programme, during which a delegation from the Republic of Macedonia visited the Slovak Republic. The Authority delivered several presentations and training activities, especially on the requested topic of physical security and object security. At the end of 2022, the Security Council of the European Space Agency (ESA) approved a security agreement between the Government of the Slovak Republic and ESA.

6.6 Distribution of security bulletins and warnings

SK-CERT has been distributing regular security bulletins and warnings since its creation. The documents contain warnings about vulnerabilities in various systems and services. They are mainly intended for the OESs and PDS, but anyone can subscribe to them for free.

Vulnerability assessments found in bulletins and alerts follow the internationally recognised CVSS 3.1 methodology used to assess vulnerabilities in software and hardware products.

Security bulletins are issued on a weekly basis and contain a list of medium and high severity vulnerabilities according to CVSS metric 3.1. Security warnings contain critical vulnerabilities and, if they have a high impact, SK-CERT also issues warnings for vulnerabilities with lower severity.

The following table shows the number of weekly security bulletins and warnings issued in 2022

	Total number of bulletins for 2022	Total number of warnings for 2022	Total vulnerabilities
JANUARY	4	11	**36**
FEBRUARY	4	28	**46**
MARCH	5	17	**47**
APRIL	4	22	**45**
MAY	5	22	**53**
JUN	4	27	**55**
JULY	4	32	**60**
AUGUST	5	23	**61**
SEPTEMBER	4	23	**46**
OCTOBER	4	23	**50**
NOVEMBER	5	21	**59**
DECEMBER	4	22	**69**
SPOLU	**52**	**271**	**629**

6.7 CyberGame 2022

In 2022, the NSA organised a cyber security competition called CyberGame. The aim of this cybersecurity game was to introduce the topic to the public in an interesting and playful way, to spread awareness about cyber security, threats and ways to protect their important data, to motivate people to dedicate themselves to this field and to look for or support talents.

The game was designed for anyone – enthusiasts, specialists, students, teachers, public servants; regardless of age, gender, occupation or education. The game ran from March 1 to May 10 and the only necessity needed to participate was an ordinary laptop and freely available tools from the internet.

The CyberGame combined technical and non-technical tasks and in total more than 50 tasks were prepared. The game was divided into 4 streams:

- malware analysis – analysis of malicious code samples. The goal was to find out how the malicious code works and to find other connections,
- Forensic analysis -players had to find digital clues,
- obfuscation and cryptography – players analysed encrypted or scrambled information,
- OSINT – open source analysis,

Each steam contained several scenarios (stories), which were added during the game, with several tasks in each scenario that logically followed after each other. The individual scenarios were graded according to difficulty. A more difficult scenario meant gaining more points. The principle of the game was to collect points for so-called "flags". The winner was the one who scored the most points. If a player used an aid, his points were reduced. There was a bonus rating for completing the entire scenario.

A total of 1,242 players registered for the game, of which 600 were actively playing. The youngest player was 12 years old, the oldest 62. A total of 452 students, 125 female players, 37 teachers and 225 players from the public administration participated in the game. The overall winner, the best female player and the best student won an study trip to a malware lab in Montreal, Canada, while other contestants in other categories won gift prizes. CyberGame won the IT Project of the Year award in 2022, the so-called Slovak IT Oscar.

6.8 Activities of the CSCCC

The Cyber security Competence and Certification Centre is a state contributory organisation with legal subjectivity, which is connected to the state budget by an annually adjusted contribution provided by the Authority in accordance with the provisions of Section 21 and Section 24 of Act No. 523/2004 on the budget rules of the Public Administration.

From the beginning of 2022, the Competence Centre fulfils the role of a National Coordination Centre (NCC) in the network of European Coordination Centres and the European Centre of Industrial, Technological and Research Competence (ECITC) under Regulation (EU) No. 2021/887 of the European Parliament and of the Council of the European Union.

In 2022, CSCCC received accreditation from the European Commission, which confirms that it has the necessary capacity to manage European financial funds. The accreditation was a necessary condition for obtaining funding for the tasks related to the performance of the NCC. Following the successful submission of a European project in the Digital Europe programme, a grant agreement between the European Commission and the CSCCC was signed at the end of 2022.

The financial value of the project is 4 million € with 50% co-financing and its duration has been set for two years starting in November 2022.

An essential part of the tasks of the Competence Centre is the performance of compliance assessment in cyber security within the meaning of Regulation No. 2019/881 of the European Parliament and of the Council of the EU on ENISA (European Union Agency for Cyber Security) and on the certification of cyber security of information and communication technologies (the Cyber Security Regulation) and later, after its adoption, also within the meaning of the Regulation of the European Parliament and of the Council on cyber resilience (The European Cyber Resilience Act – CRA).

Due to the fact that since 2020 the European Commission has delayed the approval of harmonised European certification schemes, it is currently not yet

possible to apply to the Slovak National Accreditation Service for accreditation for compliance assessment of products, processes and services in the field of cyber security according to a special regulation and according to STN EN ISO/IEC 17065. In addition to products (i.e. products, processes and services), the competence centre is already accredited for certification:

- auditors and cybersecurity managers according to a specific regulation and STN EN ISO/IEC 17024,
- integrated quality management systems, information security management, IT service management and business continuity management, according to STN EN ISO/IEC 17021.

An important prospect of the Competence Centre is to fulfil the requirements for the application for registration of an expert institute in the list of experts, interpreters and translators of the Ministry of Justice of the Slovak Republic for disciplines and industries relevant in cyber security.

The Ministry of Justice of the Slovak Republic has in 2022/806 legislative accepted the proposal of the National Security Authority to expand the expert branch to include a new branch, Cyber Security. If the Decree of the Ministry of Justice of the Slovak Republic No. 228/2018, implementing Act No. 382/2004 on experts, interpreters, is amended in accordance with the proposal, the Competence Centre has the ambition to be the first expert organisation to perform expert activities in this newly established sector.

7 LIST OF ABBREVIATIONS

CSIRT.SK – governmental unit CSIRT (Computer Security Incident Response Team)

CSCCC – Cyber Security Competence and Certification Centre

MoT SR – Ministry of Transport and Construction of the Slovak Republic MoF SR – Ministry of Finance of the Slovak Republic

MoE SR – Ministry of Economy of the Slovak Republic

MIDRI SR – Ministry of Investment, Regional Development and Informatization of the Slovak Republic

MoD SR – Ministry of Defence of the Slovak Republic

MoI – Ministry of the Interior of the Slovak Republic

MoH S – Ministry of Health of the Slovak Republic

MFA SR – Ministry of Foreign and European Affairs of the Slovak Republic

MoEW SR – Ministry of Environment of the Slovak Republic

NCC – National Cyber Security Coordination Centre

NCKB SK-CERT – National Cyber Security Centre SK-CERT

NSA – National Security Authority

DSP – digital service provider

OES – operator of essential service