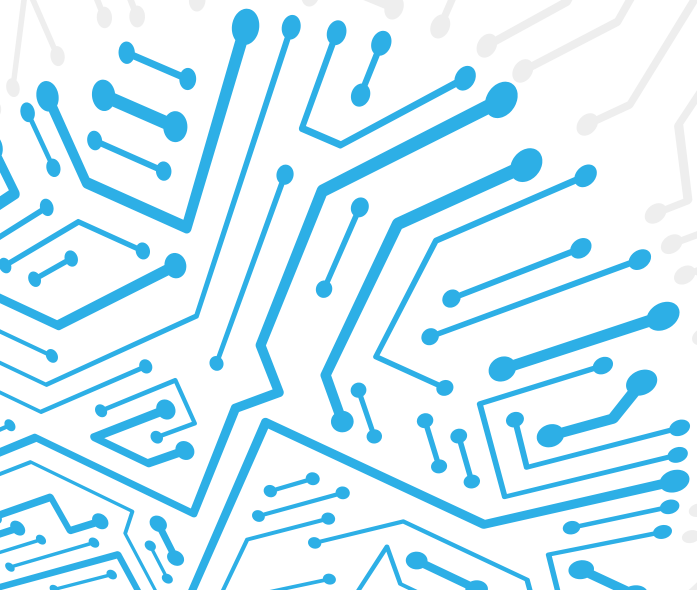
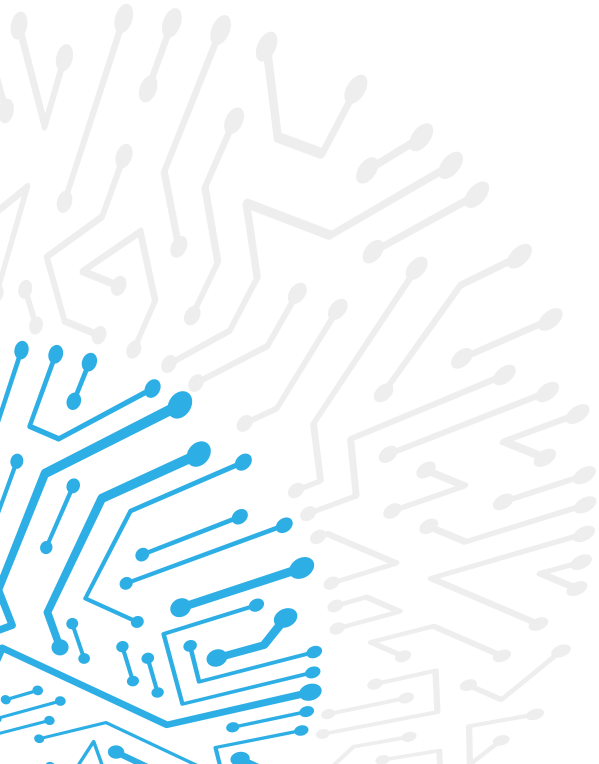
NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

2022 REPORT ON THE STATE OF CYBERSECURITY IN THE CZECH REPUBLIC





2022 REPORT ON THE STATE OF CYBERSECURITY IN THE CZECH REPUBLIC


NÚKIB
Národní úřad
pro kybernetickou
a informační
bezpečnost

Introductory Remarks by the Director

Ladies and gentlemen,

We are proud to present you with our tenth annual Report on the State of Cybersecurity in the Czech Republic. As in previous years, 2022 brought new challenges and, unfortunately, also new threats. The Russian invasion of Ukraine, which began on February 24, was undoubtedly the watershed moment, fundamentally changing the security situation on our continent. This war has had great impact on the cyberspace as well.

The mission of the National Cyber and Information Security Agency (the NÚKIB) is to provide cybersecurity for the Czech Republic. As every year, we have been working hard to fulfil this role in 2022. We continuously addressed the effects of cyberattacks and strived to prevent them. We participated in a number of domestic and international events, organized exercises, trainings, seminars, and conferences, and continuously worked to educate the public and our employees. We did all this with one main objective: to make the Czech Republic a safer place to live.

One of the major undertakings for our country in the second half of 2022 was the presidency of the Council of the EU, in which the NÚKIB participated along with several other domestic institutions. The NÚKIB succeeded in fulfilling all the three priorities set ahead of the presidency. We reached consensus among member states on the proposal for a European Parliament and EU Council Regulation setting out measures to ensure a high common level of cybersecurity in EU institutions, bodies, offices, and agencies. We prepared the Cyber Resilience Act draft and, finally, we managed to raise awareness about supply chain security of information and communications technologies.

In addition to the large number of meetings held during the presidency, we also organised a number of educational and social events in which hundreds of people from within and outside of EU attended, in-person as well as virtually. Without hesitation, I can proudly say that the Czech Republic and the NÚKIB did an excellent job, as evidenced by the reactions of our European partners. During the six months under our leadership, the EU indeed made great progress in the field of cybersecurity. At the same time, we have demonstrated that Czech institutions can work as a team. In this critically important period, during which the attention of all of Europe and allies turned to our country, the Czech Republic clearly proved a capable and reliable partner in crisis.

Just as cyberspace knows no borders, cybersecurity is boundless; and therefore, in this modern and increasingly digital world, it concerns all of us. In order to succeed in it and to keep the world and the people around us safe, we have to cooperate and communicate. Just like in the past, cooperation constituted one of the NÚKIB's main activities in the last year: from international cooperation with the EU and allied partners, domestic coordination with various entities, to cooperation with our constituents. I greatly appreciate all of our strong relationships and alliances that we have been able to build and bolster.

Finally, I would like to thank the 317 organisations that contributed to this report by completing our questionnaires. We greatly appreciate your trust and feedback. By participating, you are showing that you are not indifferent to the security of the Czech Republic and that you are determined to contribute to its promotion. Cohesion and cooperation are key ingredients to ensure the safety of all our fellow citizens.

Lukáš Kintr

Executive Summary

- **In 2022, there was a slight decrease in cyber incidents recorded by the NÚKIB from 157 to 146. However, the Police of the Czech Republic recorded an almost twofold increase in cybercriminal activities.** The activities of state-sponsored cyber actors and cybercriminal groups continue to represent the greatest threat to the Czech Republic's cyber security.

- Various types of phishing, spear-phishing, vishing, and fraudulent e-mails or attacks on availability, mainly in the form of DDoS attacks, were among the most common types of attacks during the past year. On the other hand, there was a lower incidence of vulnerability exploitation and ransomware attacks. Nevertheless, they continue to represent a relevant threat. **The NÚKIB also recorded several incidents related to the invasion of Ukraine.**

- The majority of cyber incidents registered by the NÚKIB occurred in the public sector, followed by the healthcare and private sectors. **The NÚKIB also recorded a significant, nearly twofold, increase in incidents within the critical information infrastructure, the majority of which constituted attacks on availability of services.**

- During 2022, the NÚKIB issued a total of 16 alerts and 3 warnings in response to current threats or vulnerabilities. **Some of the warnings were directly related to the risks resulting from the Russian invasion to Ukraine.**

- **A significant part of the NÚKIB's 2022 agenda consisted of preparations for and implementation of the Czech Presidency of the Council of the European Union** (hereinafter "CZ PRES"). Cooperation on the new NIS 2 Directive, which was adopted during the CZ PRES, was particularly significant. The NÚKIB worked intensively with EU and NATO partners to promote cybersecurity and develop international cooperation beyond CZ PRES as well.

- **A highly important process in terms of cybersecurity at the national level, which began in 2022, is the drafting of a new cybersecurity law, which is closely related to the aforementioned NIS 2 Directive.** As part of the preparations for this legislative change, which is expected to take effect in autumn 2024, five internal expert groups were established in which over 40 NÚKIB employees prepared a draft of the new Cybersecurity Act and its implementing regulations.

- Last but not least, the NÚKIB was also intensively involved in awareness-raising activities and held cyber exercises. A large part of awareness-raising projects took place within the education sector. Their main objective was to raise awareness of current cyber threats and create conditions for the education of future experts in the field of cybersecurity. **During the year, seven domestic and three international cybersecurity exercises took place, including a sector-focused Health Czech exercise for healthcare sector organisations.**

Table of Contents

List of Used Abbreviations

CIRC – Computer Incident Response Capability

CZ PRES – Czech Presidency of the Council of the European Union

DoS/DDoS – Denial of Service / Distributed Denial of Service

ENISA – The European Union Agency for Cyber Security

EU - European Union

ISZS – Basic Service Information system

ITU – International Telecommunication Union

CII – Critical Information Infrastructure

NATO – North Atlantic Treaty Organisation

NIS – Network and Information Security

NÚKIB– National Cyber and Information Security Agency

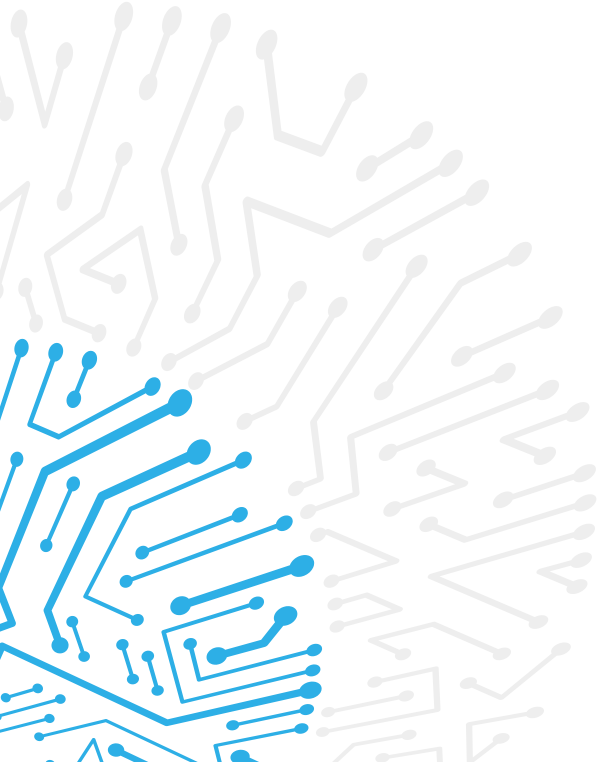
OBSE – Organisation for Security and Cooperation in Europe

OECD – Organisation for Economic Co-operation and Development

UN – United Nations

PZS – Basic Service Provider

SIS – Significant Information System



Czech Cybersecurity During 2022 in Figures

764
number of cyber incidents reported to the NÚKIB

146
cyber incidents resolved by the NÚKIB

3
severe cyber incidents resolved by the NÚKIB

2,067
security incidents resolved by CSIRT.CZ – the Czech National Security Team

1,425
phishing attacks resolved by CSIRT.CZ

18,554
cases of cybercrime and crimes committed on the Internet

504
participants in cybersecurity exercises organized by the NÚKIB

10
cybersecurity exercises organized by the NÚKIB

51,686
attendees of courses by the NÚKIB

66
subjects of critical information infrastructure

128
information and communication systems of critical information structure

193
administrators and operators of significant information systems

588
significant information systems

155
basic service providers

192
basic service information systems

About the Report

At the beginning of 2023, the NÚKIB sent out a questionnaire with 77 questions to entities regulated by the Act No. 181/2014, on Cybersecurity and on Amendments to Related Acts (Cybersecurity Act), as amended, as well as to several other key institutions and organizations that are not regulated by the Cybersecurity Act. Questions covered a wide range of topics, such as cyberattacks, cybersecurity costs, cybersecurity staffing, users, technology, and processes in place. The questionnaire was filled out by 317 entities in total, 236 of which were regulated and 81 were unregulated. From the data obtained, the NÚKIB drew information for the purposes of the 2022 Report on the State of Cybersecurity in the Czech Republic (hereinafter also referred to as the „Report"). All questionnaire data are anonymised.

Evaluation Process

The assessment of the state of cybersecurity in the Czech Republic is based on an analytical process which includes quantitative and qualitative evaluations of data from completed questionnaires, findings of the NÚKIB, information provided by its partners, and open-source information. The NÚKIB does not verify the data provided by the respondents nor validate the accuracy of their statements. The analytical conclusions in the Report are based on the premise that the questionnaire responses are not biased. Probabilistic expressions (see below) are used to express the analytical evaluation.

The Report does not provide a complete list of all activities related to cybersecurity. The purpose of the document is to describe and evaluate the threats in cyberspace that the Czech Republic faced in 2022, as well as the activities that help mitigate them.

Probabilistic Expressions Used in the 2022 Report on the State of Cybersecurity in the Czech Republic

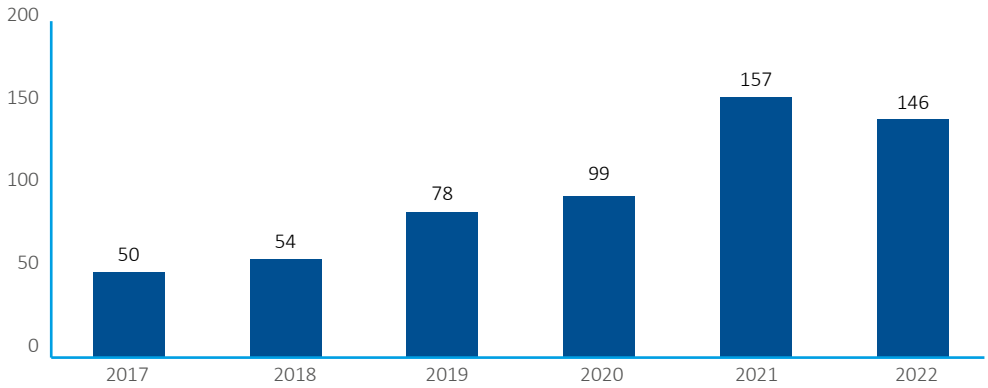
Probabilistic expressions and representation of its percentage values:

EXPRESSION	LIKELIHOOD
Almost surely	90–100 %
Highly likely	75–85 %
Highly likely	55–70 %
Cannot be ruled out/Real possibility	25–50 %
Unlikely	15–20 %
Highly unlikely	0–10 %

CZECH CYBERSECURITY IN 2022 ACCORDING TO THE NÚKIB[1]

Number of Cybersecurity Incidents in 2022 Registered by the NÚKIB

In 2022, the NÚKIB received a total of 764 reports from regulated and unregulated entities under the Cybersecurity Act, 146 of which it assessed as cybersecurity incidents and subsequently addressed accordingly. **Despite the significant increase in reporting by entities, there was a slight year-on-year decline in recorded incidents in 2022.**

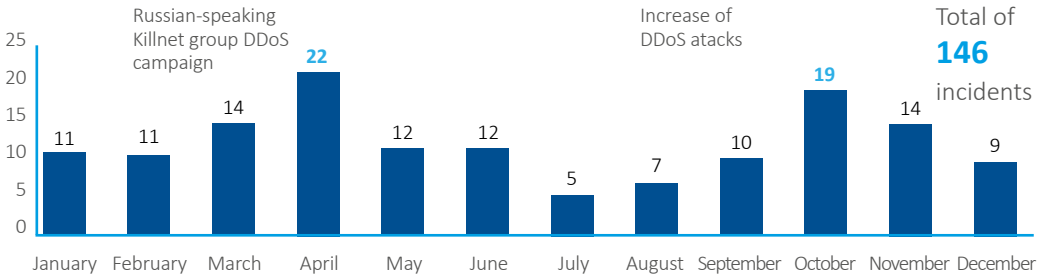


Graph 1: Number of Incidents Registered by NÚKIB

One of the possible reasons for the decrease of the number of incidents is the fact that there was no major campaign in 2022 involving exploitation of a specific vulnerability on a massive scale. In contrast, 2021 saw campaigns exploiting the ProxyLogon and ProxyShell vulnerabilities targeting the widely used Microsoft Exchange Server service. Furthermore, towards the end of 2021, the Log4Shell vulnerability was discovered. To a certain extent, proactivity on the part of the NÚKIB has also decreased (in the form so-called threat hunting, where incidents are being proactively discovered), which was primarily due to personnel limitations. Broadly speaking, it is important to establish that neither the NÚKIB nor the individual entities have the ability to detect all incidents. Especially **the most sophisticated types of attacks are very difficult to detect,** because attackers make extraordinary efforts to remain undetected. Some organisations may also fail to properly identify a cybersecurity incident or may decide not to report a detected incident to the NÚKIB. **Given the growing rate of cybercrime and incidents recorded by CSIRT.CZ, it is likely (55-70%) that the true number of incidents in the Czech Republic for 2022 is in the upper hundreds.**

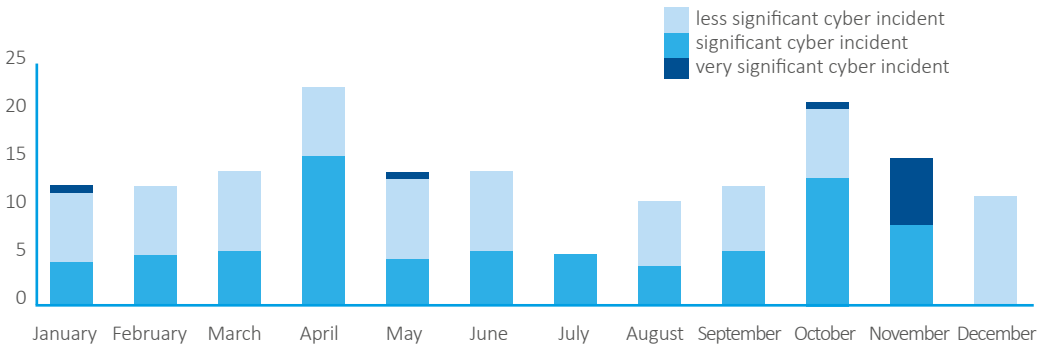
Events related to the Russian invasion of Ukraine were also reflected in the number of recorded incidents in 2022. The highest incidence was registered in April and October, which was driven by a significant increase of DDoS attacks during both months (see Graph 2). This increase was primarily due to the attacks by Russian-speaking hacktivist groups. Killnet was behind the April DDoS campaign, while Anonymous Russia claimed responsibility for part of the October attacks. **The attacks of both groups are almost surely (90-100 %) related to the Czech support of Ukraine.**

[1] *The presented information comes from NÚKIB sources and evaluations of 317 questionnaires (see the section About the Report).*



Graph 2: Number of Resolved Incidents During 2022

A key trend of the past two years is that the number of severe cyber incidents registered by the NÚKIB has been declining. On the other hand, the number of significant cyber incidents increased, while the number of minor cyber incidents decreased slightly (see Graph 3). As in 2021, the public sector was by far the most affected by cyber incidents. The health sector and the private sector followed at a greater distance. **This year, however, the NÚKIB has recorded an increase in incidents in transportation. Previous years saw only single digit values in this sector, while in 2022 there were 14 incidents.**



Graph 3: Summary of Resolved Incidents in 2022 Based on Significance

In the year 2023, Czech cyberspace will probably (55-70 %) continue to be influenced to some extent by the developments in Ukraine. Although the war affected Czech cyberspace in 2022 (see below), it did not lead to a significant increase in severe cyberattacks against Czech entities. These attacks were mainly aimed at Ukraine itself or its geographically closest allies. However, it cannot be ruled out (25-50%) that such attacks may also occur in Czech cyberspace in the coming year.

Regulated entities	Unregulated entities
72 incidents	**74 incidents**

The trend of the growing number of incidents involving unregulated entities also continued during the previous year. In 2022, the NÚKIB registered 74 of such attacks compared to 64 in 2021. **Regulated entities, on the other hand, saw a year-on-year decrease in the number of cyber incidents.**

Classification of Cyber Incidents Reported to the NÚKIB[2]

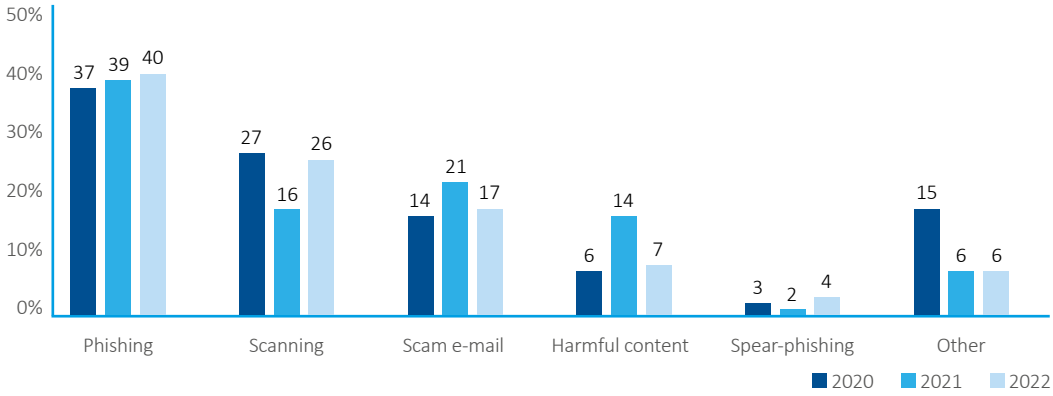
Incidents targeting availability were dominant in Czech cyberspace over the past year; this was largely because our country faced extensive waves of DDoS attacks. However, incidents targeting availability included not only DDoS attacks, but in some cases, also simple technical errors leading to system downtime. Within the availability and malicious code categories, ransomware continued to be a consistent trend, with cases present every month in 2022 except in October. However, the number of cases decreased compared to previous year which was reflected in general decrease in the malicious code category. The number of intrusions incidents also decreased. This was namely given by the aforementioned absence of campaigns exploiting vulnerabilities which occurred in 2021.

	Percentage of representation in incidents 2021		2022	Development during the year
Availability availability disruption caused by DoS/DDoS attacks or sabotage	34 %	↗	**58 %**	
Malicious code viruses, worms, Trojan horses, dialers or spyware	25 %	↘	**8 %**	
Intrusions compromising of applications or user accounts	22 %	↘	**12 %**	
Fraud phishing, identity theft or ICT unauthorized use	10 %	↗	**11 %**	
Information security unauthorized data access, unauthorized data modification	8 %	↗	**10 %**	
Intrusion attempt vulnerability exploitation attempts, login attempts etc.	1 %	↘	**0 %**	
Information Gathering scanning, sniffing, social engineering	0 %	→	**0 %**	
Offensive content	0 %	→	**0 %**	
Other	0 %	↗	**3 %**	

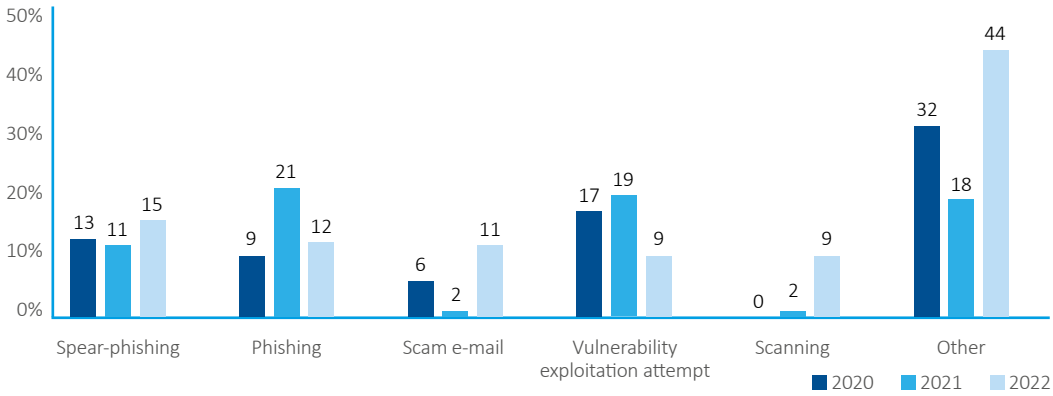
[2] The classification of cyber incidents is based on ENISA taxonomy: Reference Incident Classification Taxonomy — ENISA (europa.eu).

Incidents According to Entities: Growing Frequency and Higher Sophistication of Phishing Attacks

The most common types of cyberattacks experienced by surveyed organisations during 2022 were phishing, external network scanning, and fraudulent emails (see Graph 4). These types of attacks are less technically demanding and easy to detect; they appear regularly in our statistics. A key difference compared to the previous year has been the entities´ perception of spear-phishing, which has been declared the most serious type of attack according to the surveyed organizations (see Graph 5). This is probably (55-70 %) due to growing sophistication and persistence of attackers carrying out such attacks. **Various forms of phishing and fraudulent e-mails also continue to represent one of the most common vectors of cyberattacks globally.[3]** Overall, 68% of surveyed organizations experienced an attempted cyberattack during 2022; however, only 24% experienced a breach of confidentiality, integrity, or availability of information or services (see Graph 6).

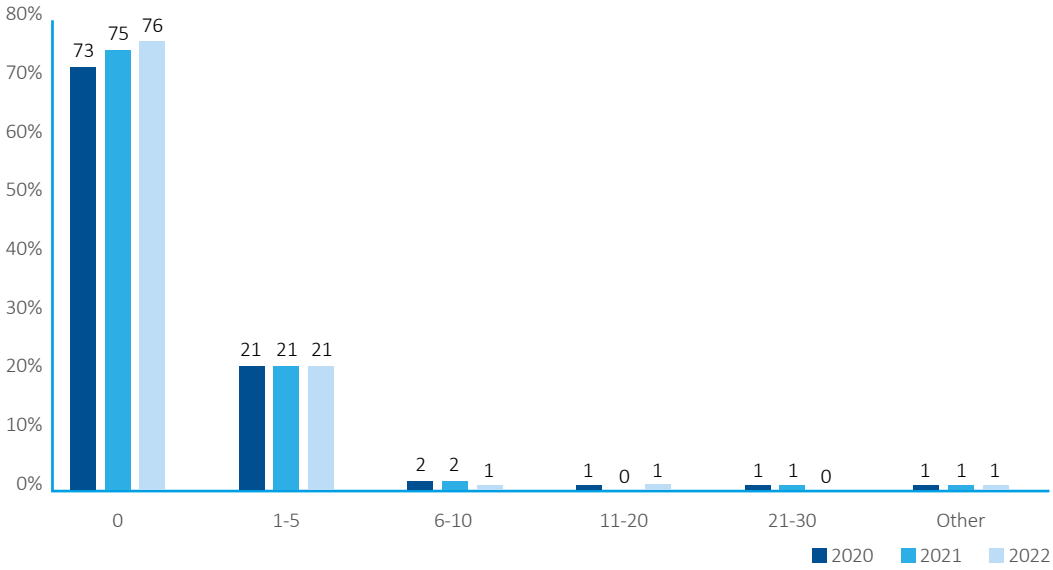


Graph 4: Most Frequent Types of Cyberattacks in 2020 - 2022 (in % of Respondents)



Graph 5: Most Severe Types of Cyberattacks in 2020 - 2022 (in % of Respondents)

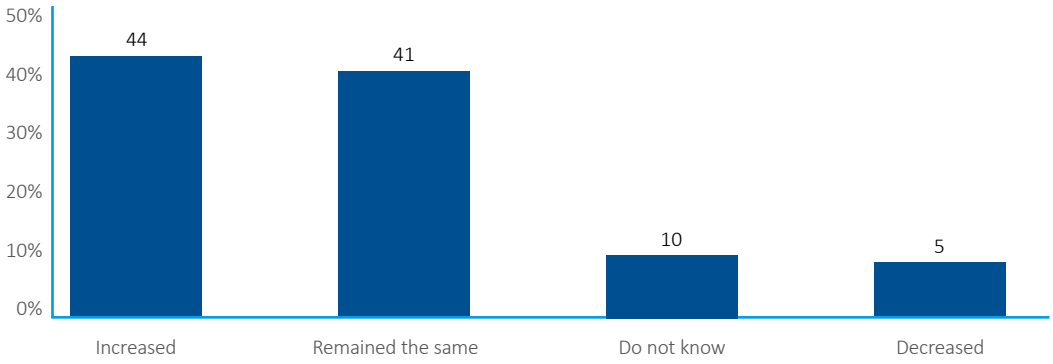
[3] *Microsoft. 2022. Microsoft Digital Defense Report 2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us*



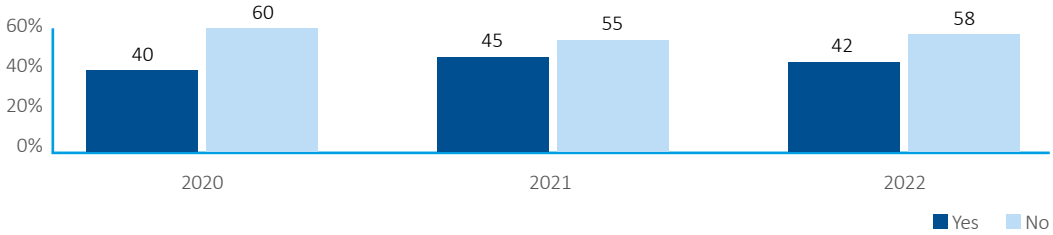
Graph 6: Number of Breaches of Confidentiality, Integrity, or Availability of Information in 2020-2022 (in % of Respondents)

Cybersecurity Funding: A Growing Number of Organizations Is Increasing Their Budgets

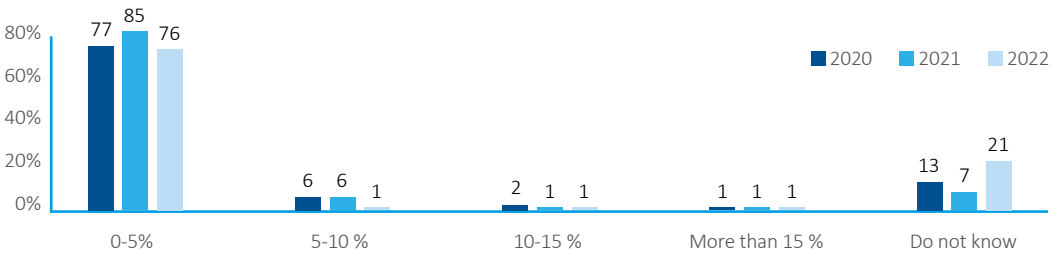
A positive trend that began in 2021 is that a growing number of organizations are increasing their cybersecurity budgets year-over-year. Despite the unfavourable economic situation in 2022 due to high inflation and rising energy prices, nearly half of the surveyed organizations increased their cybersecurity budget (see Graph 7). However, one of the drivers of these budget increases may be the current high inflation rate, as year-over-year budget levels are being assessed based on their nominal value with no regard for the inflation. **A slight majority of respondents continue to rate their funding as insufficient** (viz Graph 8). The majority of subjects spends 0-5% of its budget on cybersecurity (Graph 9), which is similar to the results in previous years.



Graph 7: Respondents' Cybersecurity Budgets Compared to 2021 (in % of Respondents)



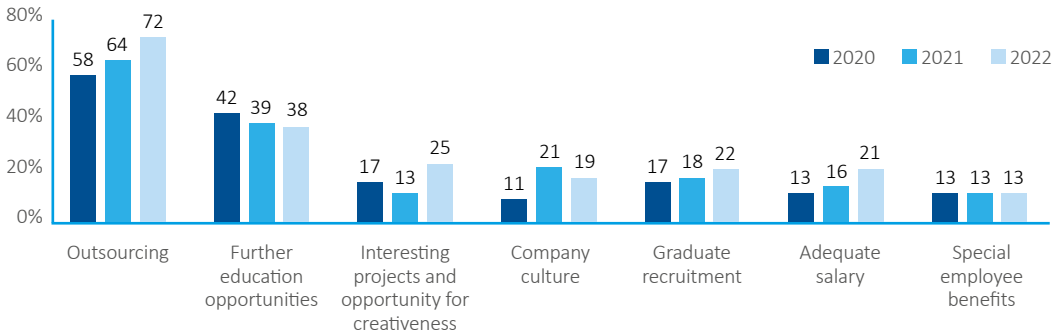
Graph 8: According to the Respondents, Has the Cybersecurity Funding in their Organization in 2020-2022 Been Sufficient? (% of Respondents)



Graph 9: Cybersecurity Budget – Share of Organizations´ Total Budget in 2020-2022 (% of Respondents)

People as Experts: Increased Outsourcing and New Opportunities for Graduates

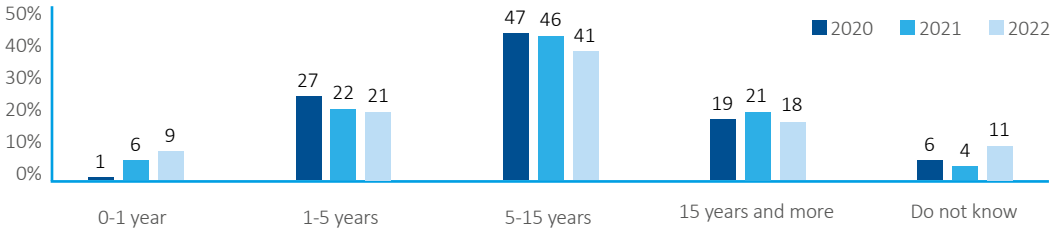
Lack of cyber security experts continued to present one of the main challenges for Czech institutions and organisations during 2022. Prospective employees' high expectations regarding their salaries are closely tied with this issue. In total, **74% of respondents openly declared that low salaries are a major factor discouraging candidates from applying for cybersecurity positions.** The questioned organisations address this issue in various ways, with three broader growing trends identified over the last three years (see Graph 10). The number of organisations dealing with the lack of cybersecurity professionals by outsourcing has increased by almost 15% since 2020, with almost three-quarters of respondents taking this measure over the past year. A gradual increase is also visible in the recruitment of graduates. One fifth of the respondents then addressed the lack of expert by raising salaries to a more appropriate level. **In the long term, outsourcing and opportunities for further development remain the most common solutions.**



Graph 10: Ways of Tackling the Shortage of Cybersecurity Professionals in 2020-2022 (% of Respondents)

There has also been a year-on-year increase in the number of respondents whose organisations are trying to offer a more interesting and creative environment for their subject matter experts. A greater emphasis on recruitment of graduates was subsequently reflected in the respondents' answers to a question mapping the average length of relevant cybersecurity work experience (see Graph 11).

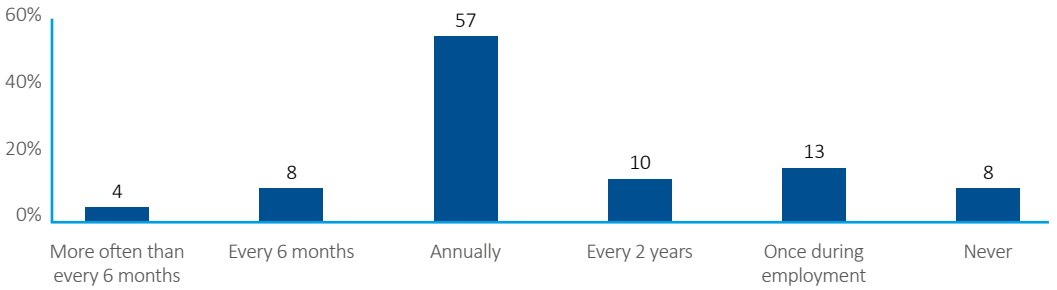
Respondents listed the following positions as the top five most difficult to fill: cybersecurity architects, network infrastructure administrators, SIEM security oversight positions, server infrastructure administrators, and cybersecurity auditors.



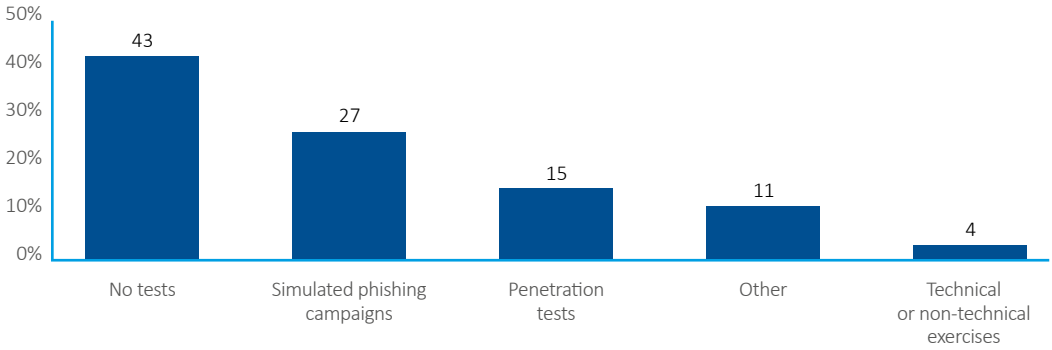
Graph 11: Average Relevant Experience of Cybersecurity Staff in Respondents' Organizations (in % of Respondents)

People as Users: Majority of Organizations Trains and Tests its Staff

Since a large percentage of cyber incidents are caused by user error or carelessness, education and testing for staff members constitutes an integral part of ensuring cybersecurity. The good news in this regard is that only less than 5% of respondents reported a complete absence of any cybersecurity training for employees. More than half of the interviewed organizations train their staff at least once a year, with nearly a tenth of organizations actively training more than once every six months (see Graph 12). **More than half of the surveyed organizations test all their staff at the same time, most often through simulated phishing campaigns.** To strengthen their cybersecurity, some organizations also use penetration testing techniques or participate in technical and non-technical exercises (see Graph 13).



Graph 12: Frequency of Cybersecurity Trainings in Organizations in 2022 (in % of Respondents)



Graph 13: Forms of Cyber Threat Resilience Staff Testing in Organizations in 2022 (in % of Respondents)

Attacks on Availability: Significant Growth of DDoS Attacks by Russian Language Hactivists

One of the consequencs of Russian invasion of Ukraine has been the increased risk of cyberattacks against the states supporting Ukraine. This is something the NÚKIB has repeatedly warned about over the past year. Although the more serious scenarios of potential threats have not materialized, the Czech Republic has been the target of a number of cyberattacks that are almost certainly (90-100 %) related to this conflict. **During 2022, several waves of DDoS attacks took place in the country, claimed by Russian-speaking hacktivists**, which targeted public sector subjects as well as private organizations.

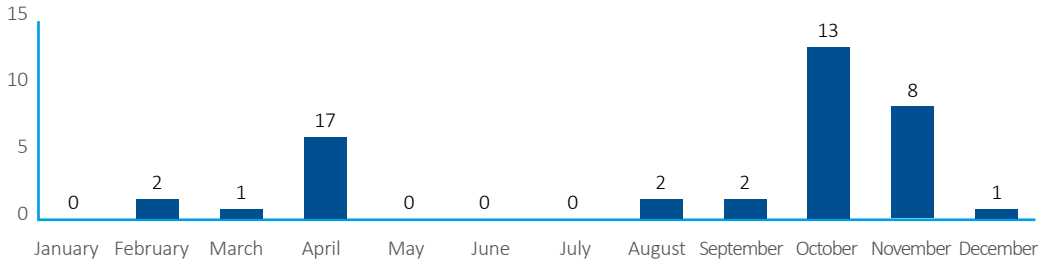
Killnet DDoS Campaign in April 2022

In April 2022, the Russian-language hacking group Killnet carried out two series of DDoS attacks against the websites of Czech entities. The first wave took place on April 19-21, affecting thirteen entities, including the NÚKIB and a number of ministries of the Czech Republic. The second wave took place on April 27, targeting nine additional subjects. The beginning of the attacks coincided with the announcement regarding ongoing repairs of Ukrainian heavy military equipment on the territory of the Czech Republic. The attackers announced their attacks on their Telegram account.

Anonymous Russia DDoS Campaign in October 2022

On October 2, 2022, the hacker group Anonymous Russia announced a wave of attacks against Czech entities on its Telegram account. Government institutions, media, banks, and airports were listed as targets. Nevertheless, the effects of the attacks were limited and only a fraction of the declared targets was hit. In the case of this campaign, efforts to establish a connection from the group's statements to any specific action by the Czech Republic as a pretext for the attack failed.

Aside for these two specific campaigns, DDoS attacks also occurred during the remainder of 2022. The monthly number of incidents caused by DDoS attacks, resolved by the NÚKIB, can be seen below (Graph 14). **According to the survey, 28% of the questioned organizations encountered an attempted or successful DDoS attack during the past year. Therefore, the number of incidents reported to the NÚKIB is almost surely (90-100 %) only a fraction of the real scope of threat activity in the country.**



Graph 14: Monthly Development of DDos Attacks Resolved by the NÚKIB

Although DDoS attacks are generally considered to be less sophisticated, **over the past year, some attackers aimed to carry out stronger and longer lasting DDoS attacks to deny the availability of services for as long as possible.** They did so by circumventing the usual mitigation measures and by using multiple DDoS attack techniques simultaneously. In the case of the aforementioned pro-Russian hacktivist groups, DDoS attacks also served as a propaganda tool. Despite their minimal impact, DDoS attacks were often heavily publicized domestically, with groups like Killnet and Anonymous Russia sharing the stories and promoting them to their domestic audiences on the social network Telegram to exaggerate their real impact. **The excessive media coverage of the attacks in the attacked countries thus paradoxically aided the goals of the attackers.**

Malware as a Service: Growing Opportunities for Cybercrime Actors

Another growing threat monitored by the NÚKIB during the past year is the so-called cybercrime-as-a-service model: the sale of tools for carrying out cyberattacks. Cybercriminal actors offer their services on black markets (especially on the so-called darkweb), which can then be purchased by actors without any deeper technical knowledge or resources. These tools include ransomware and other types of malwares, access to already compromised systems, and complex services for phishing or vishing campaigns.

Vishing-as-a-service
Offers rental of voice systems intended for carrying out of vishing attacks.

Access-as-a-service
Offers access to compromised accounts or systems.

Malware-as-a-service
Offers malware for further use in cyberattacks.

Phishing-as-a-service
Offers complex phishing services starting with detailed tutorials to e-mail templates or legitimate looking malicious websites.

DDoS-as-a-service
Offers access to infected devices connected to the Internet (so-called botnet) in order to carry out DDoS attacks.

Cybercrime-as-a-service is therefore a business model enabling virtually any person with sufficient funds to exploit tools or services for cyberattacks. This makes malicious cyber activity more easily available even for relatively unexperienced attackers. Due to the growing popularity of this model, which is capable of generating big profits, the competition within the market is growing, resulting in a wider offering of products and better affordability. That, in return, makes the provided services available to an even wider group of potential clients.

Ransomware-as-a-Service

Ransomware-as-a-service represents a rapidly developing threat. The NÚKIB has been recording ransomware attacks for a long time. Its victims span a wide range of public and private entities. **Since the end of 2019, the trend of the ransomware-as-a-service model, unique for its use of manyfold extortion, began to prevail.** In addition to the traditional encryption of data, additional layers of extortion may also include exfiltrating data and threats of publishing them, DDoS attacks to increase pressure on the victim, and contacting the victim's customers and partners to further increase pressure on the victim to pay the ransom (see Figure 1).

Figure 1: Four Levels of Ransomware Extortion (Source: the NÚKIB)

In the Czech Republic, the NÚKIB recorded 27 cyber incidents caused by ransomware during 2022, with 15% of respondents reporting an attempted or successful ransomware attack. **Ransomware, even in the form of a service, thus represented a continuing trend and threat to the security of domestic organizations in 2022.**

Phishing, Spear-Phishing, and Vishing: Growing Sophistication and Persistence

Similar to 2021, phishing, spear-phishing, and fraudulent emails comprised the most common vectors of cyberattack. The trend of increasing sophistication continued also into the last year. **The NÚKIB also registered more vishing cases,** i.e. fraudulent phone calls in which attackers attempt to gain access to the victim's systems, along with extorting login credentials, particularly online banking information. During 2022, an attempted or successful phishing attack was experienced by 92% of respondents, spear-phishing emails by 49%, fraudulent emails by 89%, and vishing by 20%. Compared to the previous year, the data show a slight increase. The NÚKIB warned about these types of attacks several times during the past year in the form of warnings (see the Box).

In reaction to phishing campaigns, the NÚKIB issued three alerts in 2022. Two of them were published in response to a vishing campaign in February and April. The perpetrators of this campaign aimed to persuade victims that their system had been compromised, which would then need to be resolved by a pretend Microsoft staff. However, the operator would instead attempt to access the victim's system through a remote access tool, used to obtain payment card details. He would also instruct the victim to confirm the two-step verification of sent payments or install a so-called keylogger on the victim's system.

- Alert to new wave of fraudulent vishing calls
- Alert to still continuing wave of fraudulent vishing calls

In August, the NÚKIB issued an alert related to a phishing campaign using the subject of social housing allowances. Fraudulent messages were spread via email and SMS messages, attempting to trick victims into sharing their banking identities with the attackers. The campaign was active for several weeks.

- Alert to phishing campaign with aim to exploit bank identity

The best defence against these attempts is the education of society, i.e. increasing people's awareness and caution and improving their ability to recognize these attempts.

92 %
surveyed organizations stated they were targeted by a **phishing attack** or a phishing attempt in 2022
(+2 % compared to 2021)

89 %
surveyed organizations stated that they were targeted by an attack or attempted attack in form of a **fraudulent e-mail** in 2022
(+5 % compared to 2021)

49 %
surveyed organizations stated they were targeted by a **spear-phishing attack** or spear-phishing attempt in 2022
(+2 % compared to 2021)

20 %
surveyed organizations stated they were targeted by a **vishing attack** or vishing attempt in 2022
(+9 % compared to 2021)

The NÚKIB is also registering a trend of increasing persistence of attackers, who often deploy automated methods of infrastructure creation to keep the campaign running even in the event of proactive interventions. The sophistication of attackers is also improving, especially the credibility of fraudulent emails and fake websites (more on this topic in the chapter: Outlook: Cybersecurity Trends in the Czech Republic for 2023 and 2024).

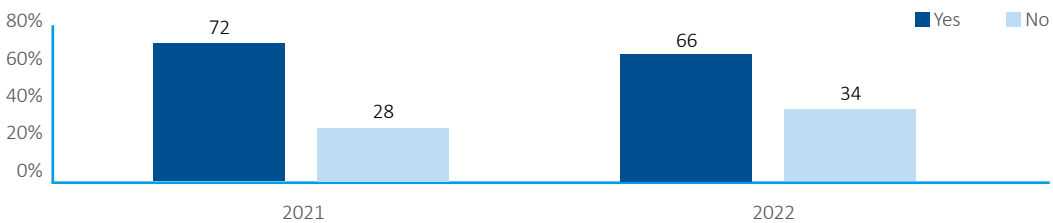
Supply Chain Attacks: Low Incidence, but with High Potential Impact

In 2022, less than 6% of surveyed institutions and organizations experienced an attempt or a successful attack through a service provider. This is an identical amount as in 2021, with this type of attack remaining among the least frequent. This is probably (55-70%) due to the combination of several factors, in particular the lower incidence of this attack type in the Czech Republic in general, low detection capability on the part of organizations and significant efforts of attackers to be undetected in the victim's systems.

However, the NÚKIB dealt with several serious cases in May of last year that highlight the need for a supplier management process. In one cyber incident that caused significant damage to the victim organization, the attacker penetrated victim's network through a compromised VPN account of their servicing company. Two more examples of poor security measures were discovered by organizations themselves, probably (55-70%) before attackers could exploit the vulnerabilities. The two organisations found that their information system supplier was storing their sensitive data on web storage without authentication.

Supplier management is one of the organizational security measures that selected entities covered by the Cybersecurity Act are required to implement. The supplier management process serves primarily to identify risks associated with the use of third-party services and their subsequent mitigation.

The year-on-year comparison of the number of respondents whose organisations manage the risks associated with suppliers shows a slight decrease (see Graph 15). Within Critical Information Infrastructure (CII), 86% of responding organisations manage these risks.



Graph 15: Does Your Organization Manage Supplier-Related Risks?
(Year-on-year Comparison, in % of Respondents)

During 2022, based on the mandate granted by the National Security Council, the NÚKIB worked on a bill aiming to significantly limit the impact of high-risk contractors on the country's most important infrastructure. While cybersecurity threats arising from technology supply chains have long been known, there is still no comprehensive legal mechanism in the Czech legal system to enable targeted assessment and mitigation of the risks arising from these threats (more in the chapter: Ensuring Cybersecurity on a National Level: Strengthening Resilience against Cyber Threats).

Cyber Threat Actors

State-sponsored and cybercrime activities in cyberspace have long been among the most serious threats to the Czech Republic's cybersecurity.

State-sponsored groups are typically highly sophisticated actors using a wide range of techniques to achieve their goals and constantly refining their tools. Russian state actors in particular represented an increased risk for the Czech Republic during the last year. **In the context of the Russian invasion, a cyberattack from early 2022 was attributed by all member states through the process of** coordinated attribution **to the Russian Federation. This attack had also indirect impact on Czech entities (see Box).**

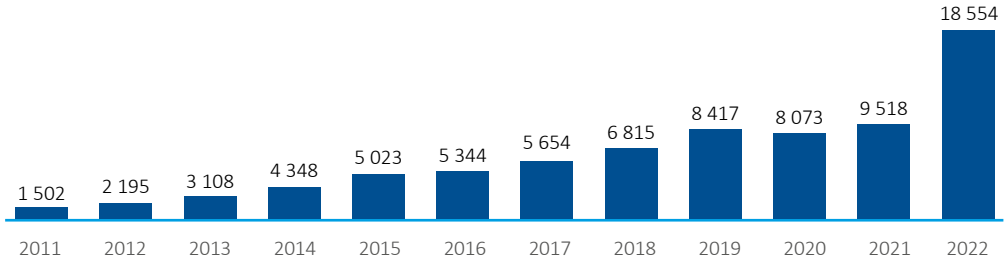
Cyberattack on Satellite Internet Provider Viasat

In the early morning of February 24, 2022, around the same time as the invasion of the Russian armed forces, a cyberattack was launched against Viasat's ground terminals providing satellite internet connectivity in Ukraine. The attack gradually limited their functionality, with a spillover effect impacting tens of thousands of users in North Africa, the Middle East and Europe, including some in the Czech Republic. Thanks to the relatively low number of Viasat users, this attack had no significant impact on the Czech Republic.

In 2022, the NÚKIB also registered a cyber espionage campaign against one of the national strategic institutions, highly likely (75-85 %) carried out by the Russian state-sponsored actor APT29 (also known as Cozy Bear, The Dukes, or NOBELIUM). **This actor is usually attributed to the Russian Foreign Intelligence Service (SVR)**. In this campaign, the email account of one of the target institution's employees was compromised. The attacker then used the account to send spear-phishing emails to over a thousand addresses of partner organizations. **The list of victims of this campaign indicates that the actor's goal was to gain access to strategic information.**

Last year, the NÚKIB also registered increased activity of pro-Russian hacktivist groups Killnet and Anonymous Russia, which carried out DDoS attacks against a number of Czech entities. These groups represent rather less sophisticated actors and the effects of their attacks have been marginal.

In general, the trend of growing cybercriminal activity continued throughout the last year. In 2022, according to the Police of the Czech Republic, a total of 18,554 offences falling under the category of cybercrime and other crimes committed in cyberspace were registered, which represents a very significant year-on-year increase of 95%. This confirms the assumption that cybercrime is a continuously growing threat, and its further growth is likely (55-70%) in the following years (see Graph 16).[4]



Graph 16: Investigated Cybercrime Cases in the Czech Republic between 2011 and 2022

[4] *Police of the Czech Republic. 2022. Development of registered crimes in 2022. https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx*

TARGETS OF CYBERCRIME ATTACKS

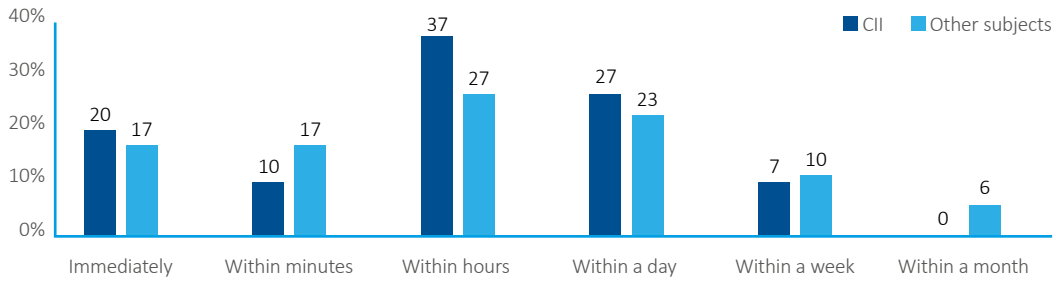
Critical Information Infrastructure: Increase of Attacks on Availability of Services

As in previous years, critical information infrastructure (CII) entities were exposed to cyberattack attempts during 2022. **The number of incidents registered by the NÚKIB in this category almost doubled.** This is a significant increase, which was probably (55-70%) due to the increase in DDoS and other service availability attacks, which made up the majority of recorded incidents in this category. The share of incidents that resulted in a disruption of availability of services remained about the same year-on-year, but in nominal terms, the number of incidents increased by about 70%. **For CII, disruption of availability can have major consequences (see Box).**

According to Section 2(b) of the Cybersecurity Act, CII is an element or a system of critical infrastructure elements in the sector of communications and information systems in the field of cybersecurity. Pursuant to Section 2(g) of Act No.240/2000 Coll., on Crisis Management and on Amendments to Certain Acts (the Crisis Act), as amended, critical infrastructure is defined as an element of critical infrastructure or a system of elements of critical infrastructure, the disruption of which would have a serious impact on national security, basic needs and welfare of the population, or national economy.

Typical elements of critical infrastructure include power plants, dams, airports, and telecommunications networks, but also strategic financial institutions and government agencies. **Disabling any of these elements may paralyse the delivery of critical services (e.g. electricity, heat, water, or pension payments) and, in extreme cases and in the event of targeted cyber sabotage, cause even physical damage.**

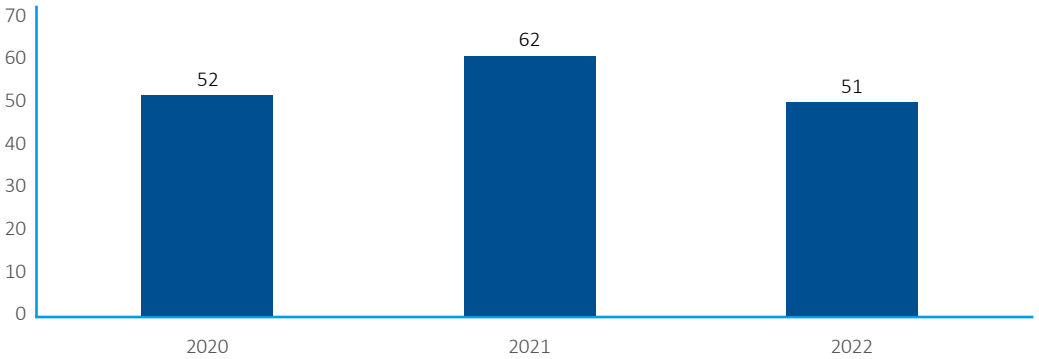
On the positive side, despite the increase in the number of attacks, there has been a year-on-year improvement in the speed of incident resolution within the CII**. In two thirds of incidents, systems were restored into full functionality within hours from compromise, with no incident taking more than a week to resolve** (see Graph 17).



Graph 17: Average Time from Cyber Incident Identification to its Resolution (% of incidents)

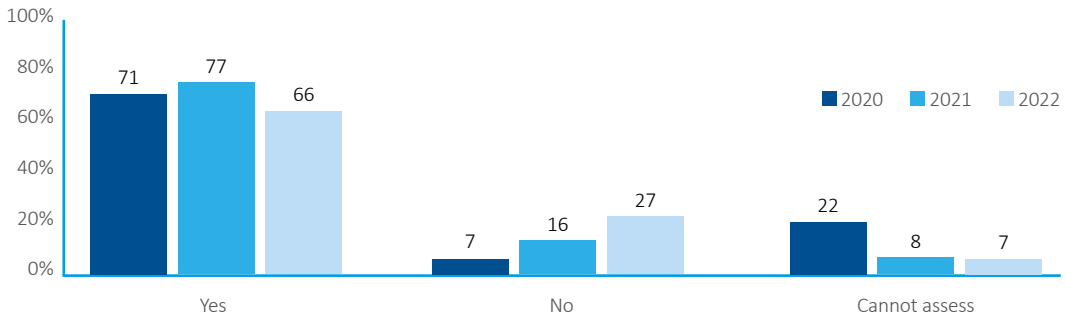
Public Sector: Decrease of Incident Numbers to Values From 2020

The public sector has traditionally been one of the most targeted sectors, and 2022 was no different. **A total of 51 cyber incidents were recorded in this sector, representing more than a third of the total.** However, the nominal and proportional representation of incidents slightly decreased compared to the previous year (see Graph 18). **The highest number of cyberattacks was aimed at data availability, which can be partially explained by several DDoS campaigns, mostly carried out by Russian-language hacktivists in connection with Czech support for Ukraine.** These attacks often targeted various government or public institutions but tended to be less sophisticated and very limited in terms of real impact.



Graph 18: Development of the Number of Incidents in the Public Sector Recorded by the NÚKIB in 2020-2022

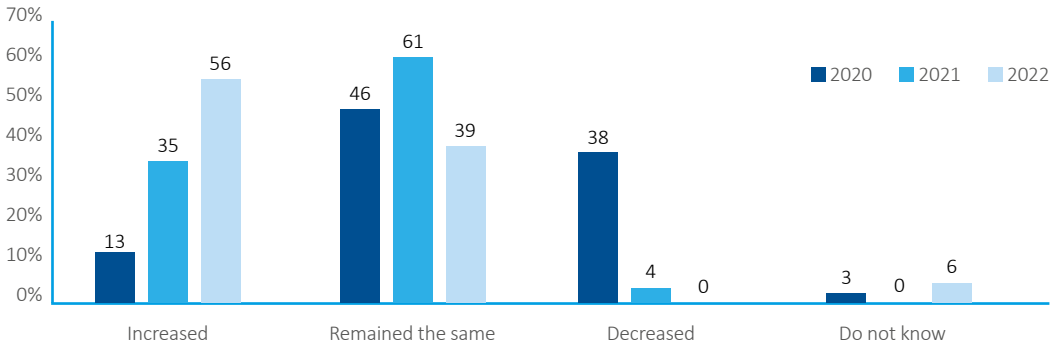
Despite the year-on-year decrease of the number of incidents, there is an increasing number of respondents in the public sector who perceive the level of their cybersecurity as insufficient (see Graph 19). This increase by more than 10% of respondents assessing the level of cyber security in a negative light may be to some extent related to the fact that 7% of respondents in the public sector also said that their organization had decreased their cybersecurity budget. Another factor may also be the serious impact of incidents on the public sector, especially in terms of damage to reputation and service disruptions, which were mentioned by nearly a one-fifth of critical infrastructure entities.



Graph 19: Do you Perceive the Level of Cybersecurity in Your Organization as Sufficient? (Comparison of 2020–2022 in %)

Financial Sector: Number of Cyber Incidents Has Doubled

The number of cyber incidents within the Czech financial sector doubled year-on-year. In 2021, the NÚKIB recorded only four incidents; last year, eight incidents were recorded. Three incidents fall into the significant incidents category. Survey shows that more than half of financial sector respondents experienced more than five cyberattack attempts during 2022; however, most of these attempts did not result in a cyber incident. **At the same time, more than half of respondents in financial institutions reported that their organization had increased the budget allocated to cybersecurity year-over-year, which, indicates a willingness to continuously invest in this area and thus improve the level of their cybersecurity** (see Graph 20).



Graph 20: How Has your Organization's 2022 Cybersecurity Budget Changed from the Previous Year? (Comparison of 2020–2022 in %)

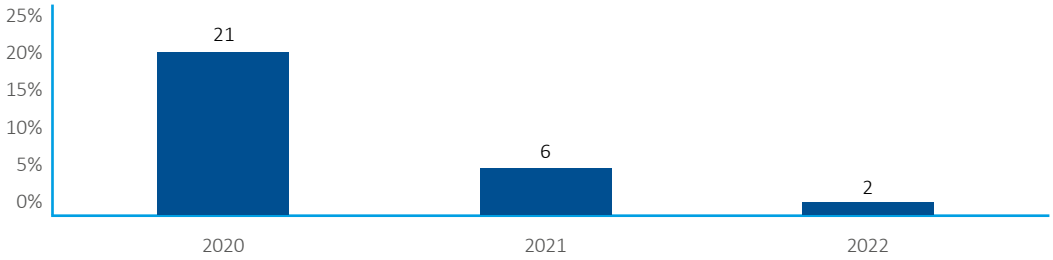
In addition to the increase of incidents described above, there was also a year-on-year increase in cyberattacks or other various forms of internet fraud against clients of financial institutions. **According to the Czech Banking Association data, cyberattacks against clients of Czech banks more than doubled, with vishing identified as the primary threat.**[5] During 2022, the NÚKIB issued several warnings related to vishing and other fraudulent campaigns using cyber tools.[6]

In response to this issue, the Czech Banking Association, in cooperation with the NÚKIB and other partners, prepared the #nePINDej awareness campaign. The campaign is available on the Kybertest.cz website and aims to increase the resilience of Czech citizens towards the most common types of fraud associated with internet banking.

[5] *Czech Banking Association. 2022. The number of cyberattacks grows dramatically and they are still more sophisticated. On that ground ČBA launches a nation-wide educational campaign #nePINdej!. https://cbaonline.cz/kybertest-2022*
[6] *NÚKIB. 2022. Threats and vulnerabilities. https://www.nukib.cz/cs/infoservis/hrozby/#1*

Industrial and Energy Sectors: New Risks Related to Smart Energy Meters

During the past year, the energy sector faced major challenges related to the impact of the Russian invasion to Ukraine and the subsequent sanctions regime and the rise in energy prices. The situation also became more severe in terms of the number of cyber incidents handled by the NÚKIB. **Compared to 2021, the number of recorded incidents increased from three to nine, while the majority consisted of attacks aimed at the availability of services or information.** On the other hand, the share of ransomware attacks, which represented a significant threat in the past two years, decreased within the energy and industrial sectors (see Graph 21).



Graph 21: Year-on-year Comparison of Recorded Ransomware Attacks or Attempted Attacks Within the Industrial and Energy Sectors (%)

The year 2022 has also brought new risks for supply chain security, especially for energy but also other industries. There is currently an ongoing debate surrounding the so-called smart meters, especially about procurement and use of secure devices (see Box). The proliferation of these components, which according to current legislation must be deployed at consumption points with demand of more than 6 MWh by 2027, means that it is necessary to consider their cybersecurity as well. **The main challenge is to ensure the security of the supply chain, because a significant number of these smart meters will be installed in the Czech Republic in the coming years and will eventually form a significant part of the energy distribution system.**

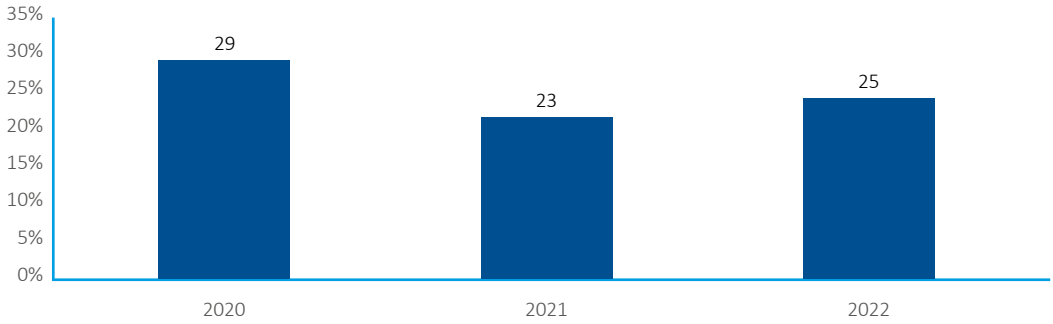
Smart Meters

Smart electricity meters are currently a relatively dynamic and expanding element of the energy distribution network digitalization. They represent an essential element of smart grids; their main purpose is to provide up-to-date information on the load on the system, to ensure better control, security, and stability of the grid, but also to provide feedback on energy consumption to end customers. However, smart meters also pose some risks, as they are relatively simple devices connected to the internet. They can therefore become the target of cyberattacks, with potential consequences including not only leaks of sensitive data, but also, in extreme cases, physical damage to the distribution network in the event of improper handling.

The potential risk of supply chain compromise exists in particular for companies based in countries whose political and legal environment requires them to cooperate with local security or government authorities at the expense of the privacy or security of the company's customers. However, a threat is also posed by companies that, through their ownership structure or business cooperation, effectively form an intermediate link in the supply chain between the Czech Republic and countries with the above-described high-risk political and legal landscape. **Both of these risks are currently monitored by the NÚKIB, which raised the issue in 2022 by means of a** warning **for domestic entities.**

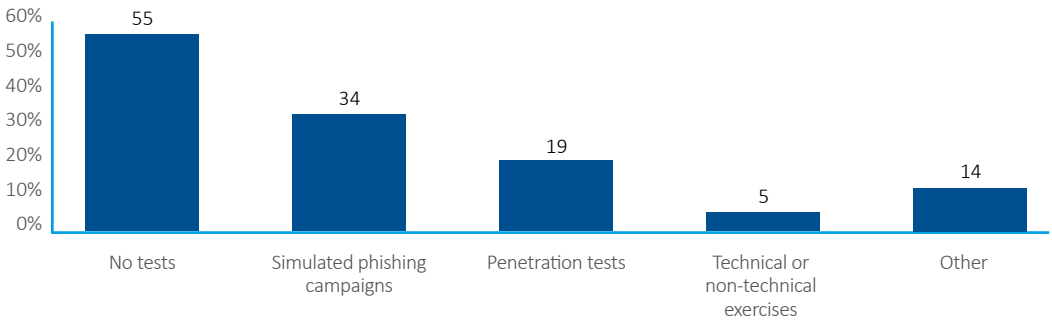
Healthcare: Ransomware Remains a Relevant Threat

The number of registered incidents within the healthcare sector increased slightly year-on-year by 3, to a total of 29 incidents. However, the NÚKIB registered a higher number of minor incidents in the healthcare sector and a 50 percent reduction in the category of significant and very significant incidents. According to respondents, there was a slight year-over-year increase in the number of organizations experiencing an attempted ransomware attack, by two percentage points. **Ransomware thus remains a relevant threat to a quarter of healthcare organizations even after the end of the covid-19 pandemic** (see Graph 22).



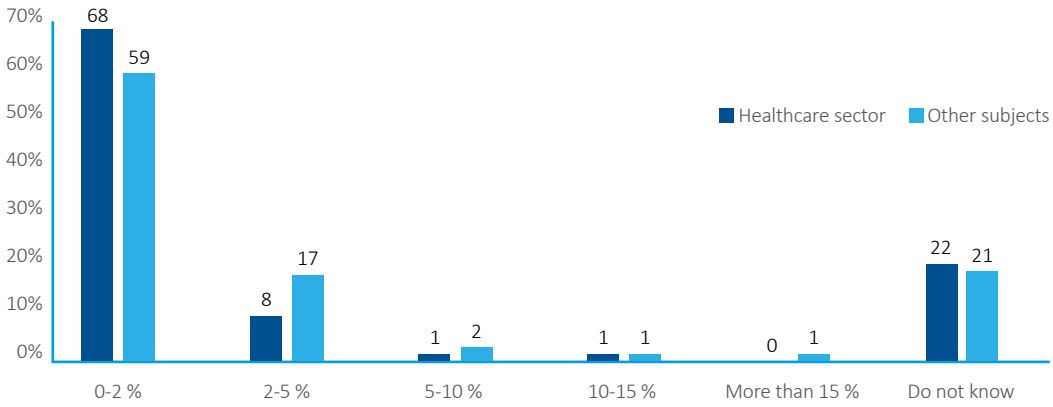
Graph 22: Share of Healthcare Sector Respondents whose Organizations Experienced a Ransomware Attack Attempt (Comparison 2020-2022 in %)

In terms of severity of different types of cyberattacks, ransomware was rated by respondents from the healthcare sector as less serious than phishing and spear-phishing attacks or fraudulent emails, which also accounted for the majority of recorded attacks. **Despite the perceived severity and the frequency of these attacks, only a third of healthcare respondents test the resilience of their staff with simulated phishing campaigns, while more than half of respondents do not test them at all** (see Graph 23).



Graph 23: Do you Test the Resilience of your Staff Against Cyber Threats? (% of Respondents)

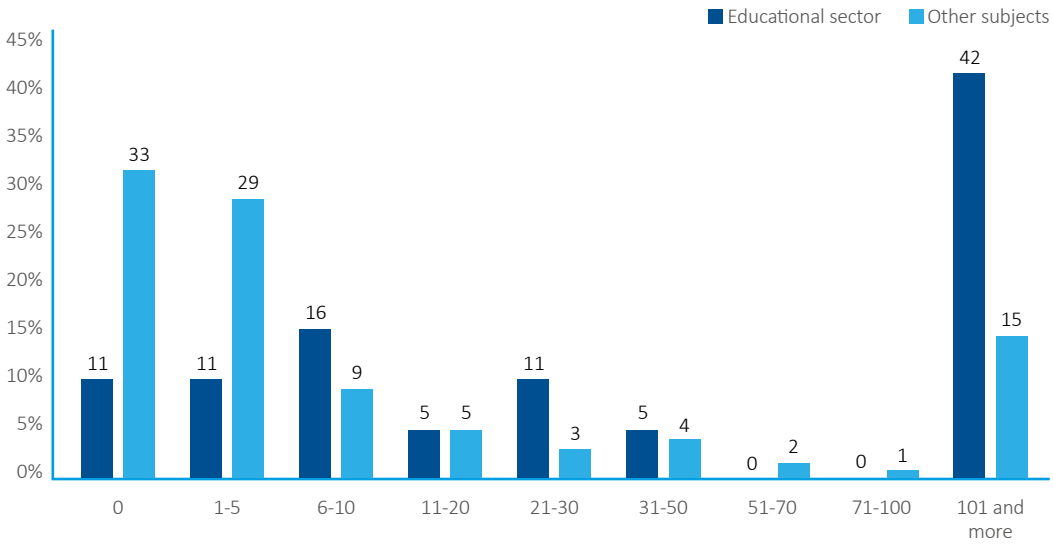
The reason for this deficiency is probably (55-70%) the long-term unsatisfactory cybersecurity funding levels in healthcare, with more than 70% of respondents assessing the level of the budget in this field as insufficient. The situation can be further demonstrated by a comparison of cybersecurity budgets in healthcare compared to other sectors, which shows that healthcare entities on average allocate lower budgets than the cross-sector average (see Graph 24).



Graph 24: What Percentage of your Organization's Total End-to-End Budget Went to Cybersecurity Expenses in 2022? (%)

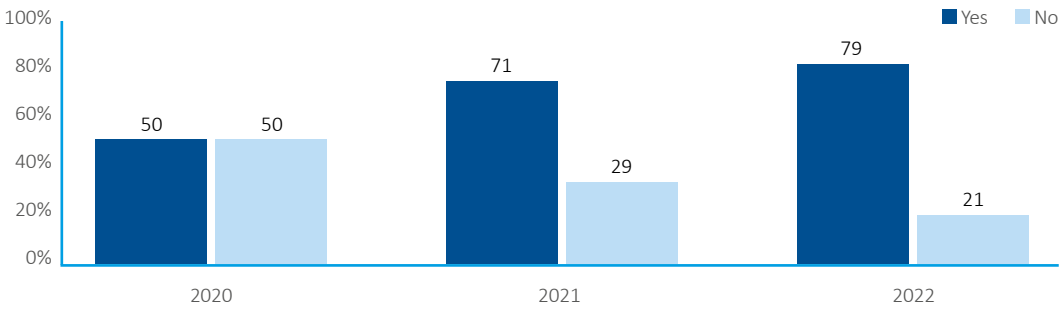
Education: Growing Emphasis on User Training

The education sector, which recorded an unprecedented increase in cyber incidents during 2021, remained an attractive target for attackers during the past year. Though the number of reported incidents decreased to nine, compared to the previous year, **respondents from education sector reported relatively high number of attempts in comparison with other sectors.** The biggest difference can be seen in the extreme values of the scale, where only one tenth of entities did not record any cyberattack attempt, while more than two fifths of the interviewed subjects reported 101 or more attempts (see Graph 25).



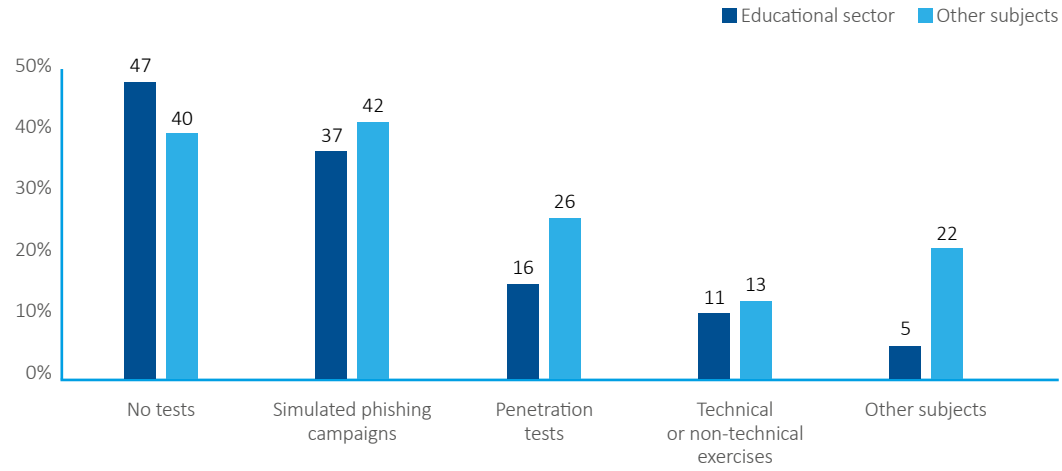
Graph 25: Comparison of Recorded Cyberattacks (Including Failed Attempts) in 2022 (% of Respondents)

The trend of phishing campaigns continued into the last year, with phishing and fraudulent emails representing almost two-thirds of the most frequent cyberattack attempts in the education sector. However, respondents further reported that approximately two-thirds of these attempts did not result in a cyber incident, which is comparable to other sectors. Since phishing attacks primarily target individual users, their training or resilience testing is generally considered the best prevention. The steady growth of the number of educational institutions that provide these trainings is a positive trend (see Graph 26).



Graph 26: Education Sector Organisations Providing Cybersecurity Training (%)

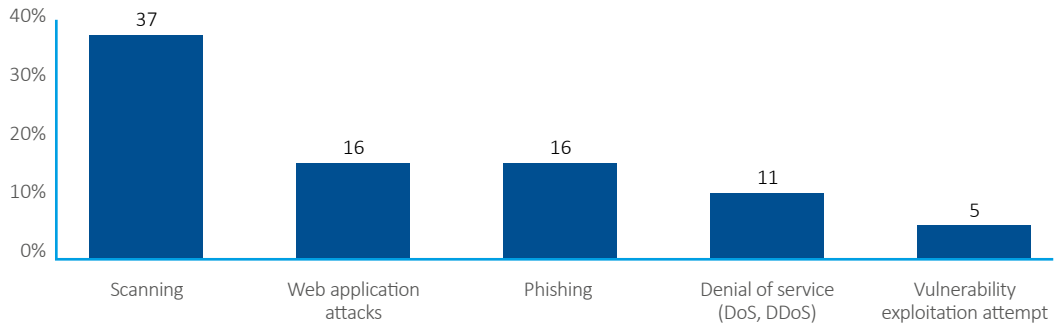
Academic research represents a valuable target for state-sponsored groups and phishing can be one of the ways for these actors to gain access to a victim's systems. User resilience testing using simulated phishing campaigns may, among other things, help reduce this risk. Despite the growing share of organizations in the education sector that train their employees, this sector lags slightly behind others in resilience testing (see Graph 27). It cannot be ruled out (25-50 %) that one of the factors contributing to this situation is the state of funds allocated to cybersecurity, which 84% of respondents in the education sector rate as insufficient, which is about one fifth more than in other sectors.



Graph 27: Do you Test the Resilience of your Employees Against Cyber Threats? (% of Respondents)

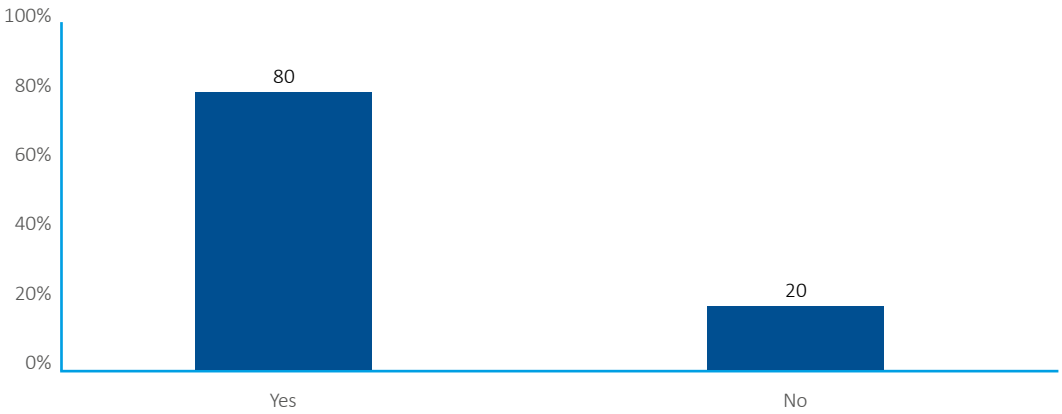
Digital Services: Targeted Through a Wide Range of Attacks

Within the Czech digital services sector (telecommunications, digital infrastructure, internet services, etc.), the NÚKIB recorded a total of eight incidents during 2022. Majority of them targeted availability of services or data. The scanning of external network ports was the most common type of cyberattack attempts according to the respondents. Compared to other sectors, scanning reached a relatively high frequency score, which can be explained to some extent by the nature of digital sector entities and their specialization. As digital services providers of internet connection, etc., they can detect automated and massive scanning of the outer perimeter of the network by attackers. **Web application attacks, phishing, DoS and DDoS attacks, and attempts to exploit vulnerabilities present additional common types of attacks** (see Graph 28).



Graph 28: Most Common Types of Recorded Cyberattacks in the Digital Services Sector (in % of Respondents)

Compared to the previous year, the share of respondents whose organizations manage supply chain security risks decreased. Exactly 80% of the surveyed respondents do so, while the majority of these entities take into account technical as well as non-technical risks in accordance with the NÚKIB recommendation for assessing the credibility of 5G network technology suppliers in the Czech Republic (see Graph 29).



Graph 29: Do You Control Risks Related to Suppliers? (% of Respondents)

MEASURES: TIMELINE OF SELECT NÚKIB WARNINGS AND ALERTS IN 2022

JANUARY

Alert Regarding an Increased Risk of Cyberespionage and Ransomware Attacks Against the Czech Republic

In January, an alert was issued about the increased risk of cyber espionage or ransomware attacks against Czech entities due to the growing tensions in Eastern Europe. Government institutions, media, and CII were considered high-risk, and the alert included an overview of specific threats and mitigation or detection measures.

FEBRUARY

Warning Against the Threat of Cyberattacks on Strategic Organizations in the Czech Republic

At the end of February, the NÚKIB issued a warning about the increased threat of cyberattacks on strategic organizations in the Czech Republic following the launch of the Russian invasion to Ukraine. The warning recommended increased vigilance against the most common attack techniques in cyberspace, urged making updates to information systems and their components, and provided a set of recommendations in the context of impending DDoS attacks.

MAY

Warning Against Using Smart Meters from Countries With Untrustworthy Legal Environments

The next warning highlighted the supply chain security threat associated with the installation of smart meters in domestic energy distribution systems. The threat lies in the use of smart metering technology from countries with untrustworthy legal environments, which may eventually cause major disruptions to the operations of the transmission system, even with possible cross-border spillover effect.

AUGUST

Alert Regarding Vmware Software Vulnerabilities

In August, the NÚKIB issued an alert following the discovery of a VMware software vulnerability that allows attackers to gain administrative access to a victim's systems without requiring authentication. The alert included a recommendation to immediately update the affected components, along with their list.

SEPTEMBER

Alert About the Microsoft Exchange Server Vulnerability

In September, two vulnerabilities (CVE-2022-41040 and CVE-2022-41082) were discovered in the widely used Microsoft Exchange Server software. Therefore, the NÚKIB issued an alert along with mitigation measures and indicators of compromise.

NOVEMBER

Alert Regarding the Increased Risk of DDoS Attacks

At the end of the year, the NÚKIB issued a warning about the increased risk of DDoS attacks, following an increase in frequency during this period, probably (55-70%) due to the joint meeting of the governments of the Czech Republic and Ukraine. The registered DDoS attacks during 2022 had only marginal impacts. Nevertheless, generally speaking, they can cause outages of critical services, such as public administration portals. Russian-language hacktivist groups were behind a significant part of these attacks.

ENSURING CYBERSECURITY ON A NATIONAL LEVEL: STRENGTHENING RESILIENCE AGAINST CYBER THREATS

Cooperation between the relevant entities, including on setting a national strategic framework, is essential to ensuring cyber security at the national level. In 2022, new developments on several important projects in this area took place.

Project BIVOJ

The mission of the BIVOJ project *(**B**ezpečný/Save, **I**novativní/Innovative, pro **V**eřejnou správu /for Public administration, **O**dolný/Resistant, **J**ednotný/Unified)* is to ensure central administration and management of security for information-sharing and communication systems and services in the Czech public sector. **The project aims to facilitate improved monitoring, communication and application of safety standards. As a result, the public sector as a whole will become more resilient, thus increasing the overall level of cybersecurity.** The project consists of several interconnected components, which are currently coordinated by the NÚKIB in cooperation with other institutions, e.g. Military Intelligence and the Ministry of the Interior.

Coordinated Vulnerability Disclosure

Coordinated Vulnerability Disclosure is a formalized process of voluntary discovery of vulnerabilities in information and communication technology (ICT) products by third parties (so-called discoverers), including notifying the owner or administrator of the ICT product of the discovered vulnerability for the purpose of security patching. **At present, there is neither a formalised and comprehensive national approach toward coordinated vulnerability disclosure nor a specific legal regulation in the Czech Republic**. Therefore, in the course of 2022, the NÚKIB designed a national framework enabling responsible and coordinated discovery of vulnerabilities for the use of public authorities as well as the private sector. In the autumn of 2022, several meetings and consultations were held with representatives of the private and public sectors to identify relevant legal and technical aspects of coordinated vulnerability disclosure. In December 2022, a national policy draft on coordinated vulnerability disclosure was then submitted for approval.

5G Network Security Measures

In February 2022, the NÚKIB, together with the Ministry of Industry and Trade, the Ministry of Foreign Affairs, the Security Information Service, the Office for Foreign Relations and Information, and the Military Intelligence, issued the Recommendation titled Doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v České republice. The Recommendation provides guidance namely for information and communication systems for the Czech critical infrastructure with regard to supplier trustworthiness. The recommendation represents the

view of the state, which is that suppliers must be evaluated not only based on the technical aspects, but also the non-technical ones – meaning the business, legal, and political environment in which the supplier operates.

Supply Chain Security

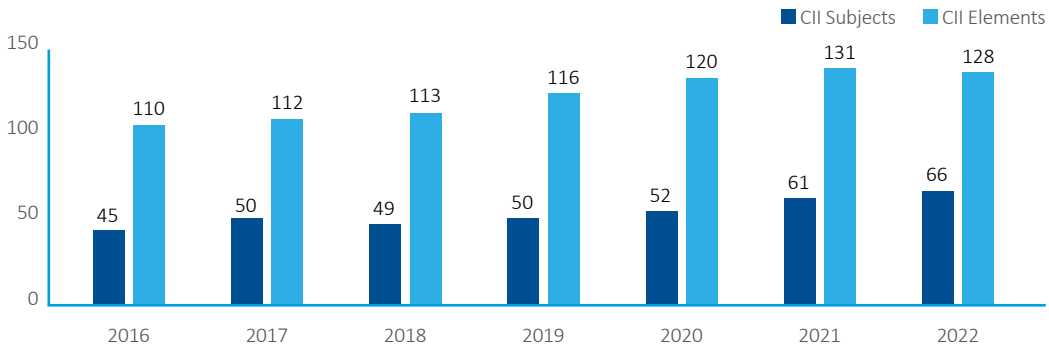
On the basis of the National Security Council assignment, in 2022, the NÚKIB worked intensively on draft legislation that would significantly limit the influence of high-risk contractors in the nation's essential infrastructure. The draft is intended to enable the state to evaluate suppliers of strategically important infrastructure. Its main objective is to increase the resilience and security of the Czech Republic and limit its dependence on potentially harmful foreign technologies. **While cybersecurity threats arising from technology supply chains have long been known, there is still no comprehensive piece of legislation in the Czech legal system to enable targeted assessment and mitigation of the risks arising from these threats.**

CYBERSECURITY LEGISLATION: DRAFTING THE NEW CYBERSECURITY LAW

Identification and Review of Critical Information Infrastructure, Critical Information Systems, and Essential Services Information Systems

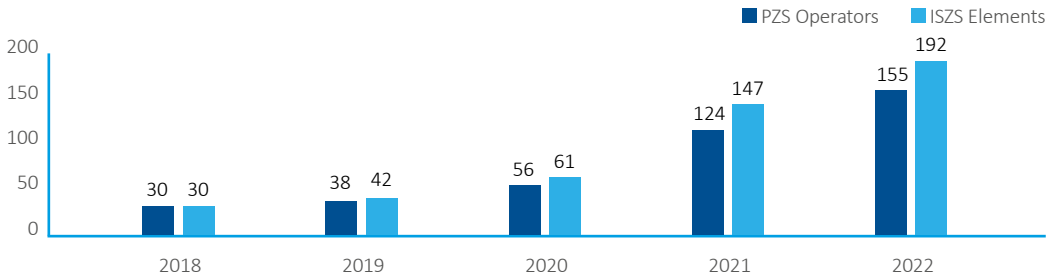
Identification of CII has been carried out by the NÚKIB since 2015 on the basis of the authorization specified in the Cybersecurity Act and the Crisis Act, in accordance with Government Regulation No. 432/2010, on criteria for determining an element of critical infrastructure, as amended. The Cybersecurity Act also requires the NÚKIB every two years to verify that the identification of CII elements is up to date. A CII element is defined as any information or communication system meeting the criteria provided in the above-mentioned regulation, which determine its importance for maintaining the vital functions of the state. The administrators of CII elements are both public and private entities.

The NÚKIB identified new and reviewed existing CII elements in 2022, during which **14 new** CII **administrators were appointed in both private and public sectors and elements of 19** CII **administrators appointed in previous years were reviewed**. As of December 31, 2022, the NÚKIB registered a total of 66 entities managing 128 CII elements (see Graph 30).



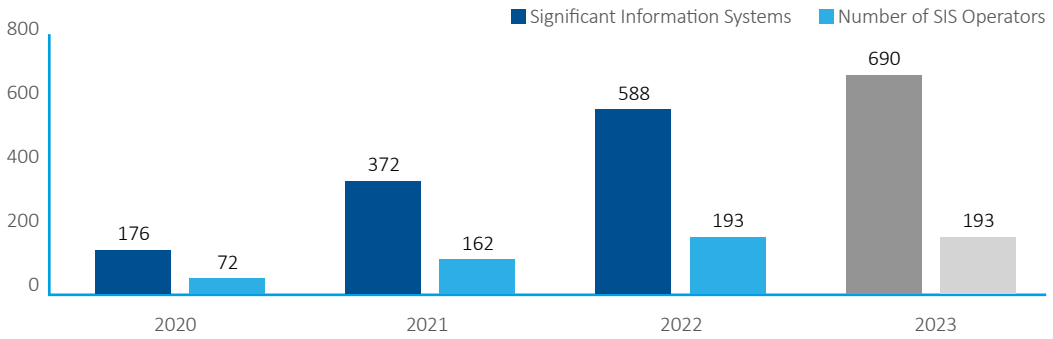
Graph 30: CII Subjects and Elements from 2016 to 2022

The process of identifying Basic Service Providers (PZS) and their Basic Service Information Systems (ISZS) also continued. In 2022, 31 new operators of basic service were identified, while 9 administrative proceedings concluded with the decision not to make this designation. Thus, the NÚKIB currently recognizes a total of 155 basic service operators, which together manage 192 basic service information systems (see Graph 31).



Graph 31: PSZ and ISZS Entities and Elements from 2018 to 2022

In 2022, another part of the Decree for Significant information systems came into effect and adding two new types of information systems to national regulation that are present in the majority of state organisations: information systems ensuring the performance of the filing service and the management of the electronic notice board. Thus, the number of significant information systems (SIS) grew from 372 (in 162 entities) to 588 significant information systems (in 193 entities). For 2023, the NÚKIB estimates an increase in the number of significant information systems to a total of 690 (see Graph 32).



Graph 32: Numbers of SIS from 2020 to 2022 and Projection for 2023

New Cybersecurity Act

The NÚKIB's most fundamental activity in the regulatory field was its work on the draft of the new Cybersecurity Law and implementing regulations in connection with Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

As part of preparations for this fundamental legislative change, which is expected to take effect in autumn 2024, five internal expert groups were established in which over 40 NÚKIB employees prepared drafts of the new Cybersecurity Act and its implementing regulations. In addition, first rounds of consultations with the experts were launched. Moreover, 25 chambers, associations, and unions representing entities that are or will be affected by this cybersecurity regulation were addressed. Every union or association was given an introduction to the future regulation and the option to participate the first round of comments. Additional negotiations and publication of complete drafts of the legislation text will took place in 2023.

In connection with the upcoming legislative changes, a specialized website focused on the NIS 2 directive and its impact on national regulation was also launched (see Nová směrnice EU o bezpečnosti sítí a informací).

European Cybersecurity Certification

In 2022, within the sector of European cybersecurity certifications based on Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA ("European Union Agency for Cybersecurity"), on the certification of cybersecurity of information and communication technologies and repealing the Regulation (EU) No. 526/2013 ("Cybersecurity Act"), the NÚKIB was established as a national cybersecurity certification body, namely by Act No. 226/2022 Coll., which amends Act No. 181/2014 Coll., on cybersecurity and on the amendment of related laws (Cybersecurity Law), as amended. In addition, the Law regulates certain aspects of the administrative procedure for so-called authorization and establishes the facts of offences consisting of violations of the obligations set out in the Cybersecurity Act.

In autumn, a strategy for securing European cybersecurity certifications was developed, focusing not only on fulfilling the tasks arising from Article 58 of the Cybersecurity Act, but also on facilitating the establishment of certification bodies and testing laboratories in accordance with the NÚKIB Development Concept. A micro website for European cybersecurity certifications was created at the turn of 2022 and 2023 (EU Certifikace). The contents of the micro website is designed to provide basic information about European cybersecurity certifications, but also resources with more detailed information.

Legislative Changes in Cloud Computing and Assessment of Security Compliance

Ministry of the Interior of the Czech Republic has been assessing cloud computing providers and cloud computing services since August 2020. The NÚKIB performs an assessment of security criteria that cloud computing providers must meet in order to be allowed to provide services for the public sector.

In 2022, the NÚKIB carried out 43 assessments in accordance with the transitional stipulations of the legal status valid until September 1, 2021. According to the legislation effective from September 1, 2021, it also carried out 46 assessments of cloud computing providers on their ability to ensure the basic level of protection of confidentiality, integrity, and availability of information in the public sector institutions. Finally, 27 assessments evaluating the aspects such as public order, security, and compliance with the rights of third-party persons were also completed.

SUPERVISORY ACTIVITIES OF THE NÚKB IN 2022

Audit and inspection activities carried out by the NÚKIB in 2022 were particularly affected by the escalation of the global geopolitical situation. Therefore, the NÚKIB focused its audit and inspection activities, among other things, on the most critical state administration systems, auditing their business continuity management.[7] In addition, a tailored table-top exercise covering this area was offered and delivered to the aforementioned organisations.

A total of 20 audits and inspections were carried out in 2022 in accordance with Decree No. 82/2018, on security measures, cyber security incidents, reactive measures, filing requirements in the field of cybersecurity and data disposal (Cybersecurity Decree), as amended. As a part of a routine inspection and audit, approximately 150 control points are inspected, while four to six NÚKIB staff members are involved in this activity, depending on the size of the entity, the complexity of the systems being audited, and other conditions requiring specific expertise or personnel of the NÚKIB. Typical inspection or audit takes approximately two to three months from start to finish.

The Most Frequent Shortcomings Identified During Inspection and Audit

- The cybersecurity assurance system in place does not meet the requirements of interested parties;
- Entities do not sufficiently manage resources and risks related to cybersecurity;
- Security policies and documentation are not put into practice or are not being updated;
- Entities do not sufficiently manage risks related to suppliers;
- Use of out-of-date hardware and software which is no longer supported by manufacturers and lack management of related risks;
- Shortage of cybersecurity experts;
- Insufficient education of employees and persons responsible for cybersecurity;
- Improper segmentation of communication network.

[7] *Business continuity – readiness to react to critical situations and ability to minimise eventual effects of such a situation.*

CYBERSECURITY EXERCISES: CZ PRES AND HEALTH CZECH

National trainings	Number of participants	International trainings
7	504	3

The year 2022 was marked by the preparations and subsequent implementation of CZ PRES. The NÚKIB organised two non-technical cybersecurity trainings aimed at preparing selected employees of the Office of the Government of the Czech Republic and other relevant authorities involved in CZ PRES preparations for a realistic crisis situation in the field of cybersecurity. The training focused on testing the crisis communication processes and channels set up for CZ PRES, also with regard to informing EU partners. The trainings also helped map the conditions of CZ PRES preparations and reveal some potential weak points.

International exercises also took place in 2022. Locked Shields 2022 was the first one. **At this most comprehensive cybersecurity exercise in the world, organised by the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, a joint team of Czech and Slovak cybersecurity specialists earned 5th position.** On behalf of the Czech Republic, the joint team included representatives of the NÚKIB, CIRC of the Ministry of Defense, EG.D, RedHat, CZ.NIC, Česká Spořitelna and other experts from the Czech security community. **Additional benefit of this training was the opportunity to deepen cooperation with our Slovak colleagues, which will carry on beyond the scope of the exercise.**

Cyber Coalition is another international cybersecurity exercise held regularly by NATO. In the Czech Republic, the NÚKIB is in charge of coordinating the civil part of the exercise, while the Command of Cyber Forces and Information Operations oversees the military part. The name of the exercise underscores its goal to support a strong community and mutual cooperation. This is achieved through scenarios that not only contain technical challenges, but also encourage individual states to work together and develop a shared situational awareness. Unlike the Locked Shields exercise, there is no formal winner; the exercise is all about cooperation, coordination, and communication in the context of dealing with a crisis emanating from cyberspace.

At the end of 2022, a second non-technical cybersecurity exercise named Health Czech 2022 focusing on the healthcare sector took place. The exercise was organized for healthcare organizations designated as basic service providers. Representatives from each entity answered questions in teams based on a prepared scenario and together discussed various aspects of cybersecurity. In addition to the teams representing health care institutions, the exercise was attended by representatives of the NÚKIB and other invited institutions (Office for Personal Data Protection, Police of the Czech Republic, CZ.NIC) which are also relevant to the management and resolution of such crises. To make the exercise more realistic, media representatives were also present to communicate with the participants about the escalating crisis to simulate a real crisis.

Future Trends of Cybersecurity Exercises: An Outlook

The NÚKIB will continue to focus on the development of the „train-the-trainer“ concept, which aims to provide support to entities in the form of consultations and workshops as they prepare their own cybersecurity exercises. This will soon be a necessity, especially in the near future following the NIS 2 Directive coming into effect, as there will be a significant increase in regulated entities and, therefore, also a significantly higher number of potential exercise participants.

AWARENESS-RAISING AND EDUCATION IN THE CZECH REPUBLIC: POSITIVE DEVELOPMENTS IN THE EDUCATION SECTOR

Cybersecurity education, awareness, and prevention were important society-wide issues throughout 2022. The need for citizens of the Czech Republic to navigate digital technologies and to be safe in the online world across all social groups, whether at work, during studies, or leisure, continued to resonate. **Beyond the usual education of public administration employees, trainings were also provided to employees of organisations involved in the realization of 2022 CZ PRES.**

NUMBER OF GRADUATES OF NÚKIB E-LEARNING COURSES	
Dávej kyber!	40 592
Šéfuj kyber!	603
Kyber nemocnice!	9 641
Bezpečně v kyber!	850

Raising Awareness in the Education Sector

Cybersecurity education at the elementary and secondary school level has been showing a positive trend for several years. In 2022, the revised education framework for elementary education and secondary vocational schools was implemented. The changes aimed to introduce new informatics and digital skills into teaching. **In addition, work on the so-called major revision of the Framework Curriculum for Primary Schools continued, in which cybersecurity will be taught as part of digital skills.**

Cybersecurity pilot testing is continuously taking place at selected high schools. For example, a trial testing of cybersecurity education according to the school educational program and a trial verification focused on the recognition of international ICT certification standards within the profile part of the graduation exam.

At universities, the trend of a slight increase in the number of students attending information and communication technology programs has continued into 2022. However, there is an insufficient increase in the number of cybersecurity-focused study programmes being prepared or opened, presenting a negative trend in this area.

In cooperation with the Ministry of Education, Youth and Sports, a course on cybersecurity basics for teachers was developed. It serves to help teachers recognize the risks associated with the internet and to make online teaching more secure.

Safe Internet Festival 2022

During the European Cybersecurity Month, the NÚKIB organised the Safe Internet Festival. A total of 34 partners from the non-profit and private sectors participated in the festival and prepared a total of 37 activities for various target groups. The NÚKIB participated in the realization of 15 activities. The festival received media support from the Czech Radio (Český Rozhlas) stations, and educational spots were broadcasted in October on the CRo Radiožurnál, CRo Dvojka and CRo Vltava stations. **The festival included the release of a cybersecurity course for seniors (SENIOR tool), which aims to help them identify malicious and dangerous emails.** As part of the festival, a so-called elevator campaign aimed at the medical staff in hospitals took place. 51 hospitals and health centres participated.

Education Within the Healthcare Sector

Following an earlier analysis, the NÚKIB supplemented online education for the healthcare sector with the course Start Cyber!. At the same time, the content and design of the Dávej kyber! course was updated for healthcare. Both courses were attended by 9641 employees from 27 hospitals and health centres. This is 5051 more trained persons than in 2021.

CyberCon 2022 Conference

In September 2022, the NÚKIB organised the eighth annual CyberCon Brno conference at the Scala Cinema and the Faculty of Social Studies of Masaryk University in Brno. The main goal of the conference is to provide space for connecting the public, academic, and private sectors in the field of cybersecurity. During the three-day programme, 500 participants from the professional and general public listened to lectures and discussions reflecting technical, political, and legal aspects of cybersecurity. **A new addition to this year's conference was the workshop day, during which participants had the opportunity to solve problems and challenges related to cybersecurity first-hand.** During the first day of the conference, the second iteration of the Study Cyber! school fair for primary and secondary school students took place.

The second day of the conference was dedicated to the latest developments in regulation. Experts presented the forthcoming NIS 2 Directive, risk analysis, and shared key findings from cybersecurity audits. During the final day, strategic perspectives on the diverse challenges in cybersecurity were presented. There was also a political discussion in which members of the Parliament of the Czech Republic discussed cybersecurity funding or the role of the state in ensuring cybersecurity.

The conference recording is available at www.cybercon.cz.

INTERNATIONAL COOPERATION: CZ PRES AND THE NIS 2 DIRECTIVE

Developments in the field of cybersecurity in the Czech Republic is largely connected to developments abroad and decisions made not only at the EU level, but also by international entities. The Czech Republic actively represented a number of international organizations and integration groups, especially in the EU, UN, NATO, OECD, OSCE, and ITU.

European Union

In the area of international cooperation, the year 2022 was particularly influenced by CZ PRES, which the Czech Republic took over for the second time in its history on July 1, 2022 for a period of six months. Therefore, the first half of 2022 was primarily dedicated to intensive preparations both in terms of content and organization and included a number of negotiations with partners at the national and EU level.

Starting with the beginning of the Presidency, the Czech Republic worked on a number of legislative and non-legislative documents in the area of cybersecurity. **A general approach of the EU Council was reached (a common position of all member states) on the proposal for a Regulation laying down measures to ensure a high common level of cybersecurity in the institutions, bodies, offices, and agencies of the Union.** The draft regulation aims to increase the level of cybersecurity of EU entities, and thereby strengthen security across the EU. **Negotiations have also begun on a draft of the Cyber Resilience Act[8] which sets out cybersecurity requirements for a wide range of products with digital elements to ensure their cybersecurity throughout their lifecycle.** National partners within the government as well as representatives of the private sector from areas which will be most affected by the regulation were consulted in autumn because the regulation will have a significant impact on the market for products containing digital elements.

In addition to these legislative proposals, the Czech Republic also focused on strengthening the security of the information and communication technology (ICT) supply chain. The main success in this area was the adoption of the Council's conclusions on the security of the ICT supply chain, which were initiated and negotiated at the EU Council by Czech representatives. By adopting these conclusions, all 27 member states confirmed the importance of ICT supply chain security and the need to strengthen it across the EU through the proposed steps. This is an important milestone for cybersecurity. However, several other issues were addressed at the EU Council, including, for example, a number of initiatives in the field of cyber diplomacy, where the NÚKIB worked closely with the Ministry of Foreign Affairs.

The adoption of the NIS 2 directive was of fundamental importance for cybersecurity at the EU level and for the future design of national regulation. The contents of the Directive were negotiated in the first half of 2022, during the French Presidency of the EU Council. **The final text of the NIS 2 Directive following language revisions was then adopted during the CZ PRES, at the end of 2022. The Directive is to become part of EU law within 21 months of coming into effect, meaning no later than October 2024.**

[8] *Cyber Resilience Act*

In addition to the activities of the Council of the EU, CZ PRES was also reflected in the work of several expert groups in the field of cybersecurity, which the NÚKIB chaired and organised during this period.

During CZ PRES, the NÚKIB held many events in the Czech Republic and abroad. **The most important event in this respect was the two-day EU Secure and Innovative Digital Future Presidency Conference,** which the NÚKIB organised together with the Ministry of Industry and Trade and the Office of the Government, in coordination with the Ministry of Foreign Affairs.

EU Secure and Innovative Digital Future Conference

The first day of the conference, called Prague Cyber Security Conference 2022, was organized by the NÚKIB, continuing the tradition of the Prague 5G Security Conference held in previous years. It was attended by over 500 experts in the field of cybersecurity from more than 80 countries, in-person as well as virtually. Speakers included Czech and foreign representatives of governments and the public sector, international organizations such as the EU and NATO, as well as various think tanks. The main topic of the day was the issue of securing the ICT supply chain and the challenges it brings.

The second day of the conference, entitled Towards a Secure and Innovative Ecosystem, was held under the auspices of the Ministry of Industry and Trade of the Czech Republic and the Office of the Government of the Czech Republic and focused on the security of new technologies, such as artificial intelligence or the issue of secure data flows within the EU and beyond.

In addition to the conference and a number of working meetings of expert groups, the NÚKIB also organized several educational and social events, all with participation of foreign partners from member states and EU institutions and beyond.

Other International Organizations

In the past year, the Czech Republic actively participated in the meetings of the UN Open Working Group on the Security of Information and Communication Technologies (OEWG), in which, along with other liberal democracies, it helped prevent the efforts of authoritarian regimes to strengthen state control over the administration of the Internet and online content and to limit human rights in cyberspace. In the long term, the Czech Republic has been promoting an open, free, safe, stable, and accessible cyberspace. Together with Microsoft and the CyberPeace Institute, the Czech Republic also participated in the international project Protecting the Healthcare Sector from Cyber Harm aimed at protecting the healthcare sector. It concluded with a set of recommendations issued in the form of a Compendium presented on the sidelines of the third OEWG meeting in New York.

In cooperation with other like-minded countries, the Czech Republic participated on the development of cyber capabilities in third countries. In particular, it has implemented projects in Bosnia and Herzegovina, Moldova, Indonesia, Senegal, and Ghana.

The NÚKIB also actively participated in the activities of the informal ICT security group at the OSCE. This year, among other things, the NÚKIB was involved in the review of a new e-learning course on coordinated vulnerability disclosure policy and spoke at a side-event on national practices in dealing with cyber incidents.

OUTLOOK: CYBERSECURITY TRENDS IN THE CZECH REPUBLIC FOR 2023 AND 2024

Threats for Energy Industry and Transportation

One of the last year's prominent trends was the growing interest of malicious attackers in the energy and transportation sectors. Importance of such threats significantly increased with the beginning of the Russian invasion of Ukraine and related events, which was soon exploited by state or state-sponsored actors, as well as cybercriminal and hacktivist groups. **It is probable (55-70%) that more or less serious attacks on entities in the energy and transport sectors in the forthcoming period will take place.** The risk of such attacks will be highly likely (75-85%) growing as a result of political decisions and other developments associated with the Russian-Ukrainian war.

Persistence of Campaigns

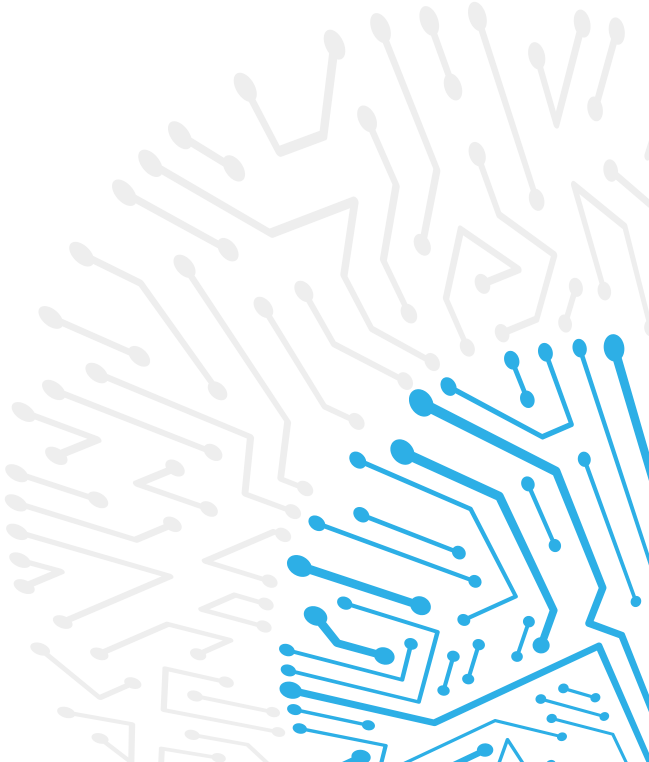
In 2022, the Czech Republic faced several persistent campaigns. The first case involved vishing, which was used to make users install remote administration software on their computers. The second persistent campaign was phishing distributed via text messages targeting bank identity and subsequent theft of funds. Both campaigns were notable due to persistence of the attackers, who continued their attacks despite active interventions by various institutions. **This shows a trend where attackers are deploying more automated methods of infrastructure creation to keep their campaign running even in case of proactive interventions. We are also observing and expecting to continue the trend of growing sophistication of attackers, especially with regard to credibility of fraudulent emails or websites used in attacks.**

Ransomware

The NÚKIB records ransomware incidents almost every month, and this trend will almost certainly (90-100%) continue in the coming years. Ransomware offered as a service (ransomware-as-a-service), which usually operates on the basis of multiple extortion (including data exfiltration, the possibility of data publication/sale or other activities aimed at increasing the pressure to pay the ransom), has become the predominant form. **Although ransomware is primarily the domain of cybercriminal groups, it cannot be ruled out (25-50%) that selected countries under sanction mechanisms will resort to using it as well, either for financial gain or to cover up their true destructive or cyberespionage goals.** There is also a real possibility (25-50%) of cooperation between non-state and state actors, with non-state actors gaining funding through this activity and state actors gaining access to exfiltrated information along with a higher level of plausible deniability.

Cyberattacks Against National Strategic Institutions

In the long term, the public sector, including strategic institutions of the state, is the most affected one, and it is almost certain (90-100%) that this will continue to be the case in the foreseeable future. In addition to the possibility of gaining valuable intelligence, attackers' motivations may also be influenced by the geopolitical situation. **For the Czech Republic, significant factors include primarily the Russian invasion to Ukraine and the Czech support for the invaded country together with its active membership in the EU/NATO.** It also cannot be ruled out (25-50%) that selected institutions are being compromised over a long period of time, and that the attacker's penetration was not identified due to the high sophistication of the attackers.



MEETING THE GOALS OF THE NATIONAL CYBER AND INFORMATION SECURITY RESEARCH AND DEVELOPMENT PLAN FOR 2022

To fulfil the objectives of this plan, the NÚKIB organized three meetings of the Platform for Research and Development in Cybersecurity, whose members are state administration authorities, academic and research institutions, and representatives of the private sector. The first meeting took place on the premises of the Technology Agency of the Czech Republic, and the second one at the Technical University of Ostrava. Both meetings focused on strengthening cooperation in the field of research and development. The third meeting was held at the Faculty of Informatics of Masaryk University and focused on current trends in the field of cryptography and the development of quantum technologies.

The NÚKIB further supported greater involvement of the user community in the research, development, and innovation support system in cybersecurity, including strengthening the ability to put results into practice. Along with departments of the Police of the Czech Republic and the Army of the Czech Republic, the NÚKIB has supported several research projects funded by public tenders of the Ministry of the Interior from the position of application guarantor. As part of international project initiatives, the NÚKIB became a member of the consortium of the project led by Masaryk University called Cyber-security Excellence Hub in Estonia and South Moravia (CHESS), whose goal is to develop research and innovation cooperation of the South Moravian Region with Estonia in the field of cybersecurity.

In 2022, the NÚKIB continued to build an information basis in the field of cybersecurity research and development. Newsletters reporting on the news in the area of science and research as well as new technologies in cybersecurity are regularly published on the NÚKIB website. By the means of scientific diplomacy, the NÚKIB organised a video conference meeting between representatives of academia and their Israeli counterparts with the aim of establishing closer cooperation leading to possible preparation of an international research project. The NÚKIB also provided several informal consultations regarding the possibility of drawing funds from EU framework programs.

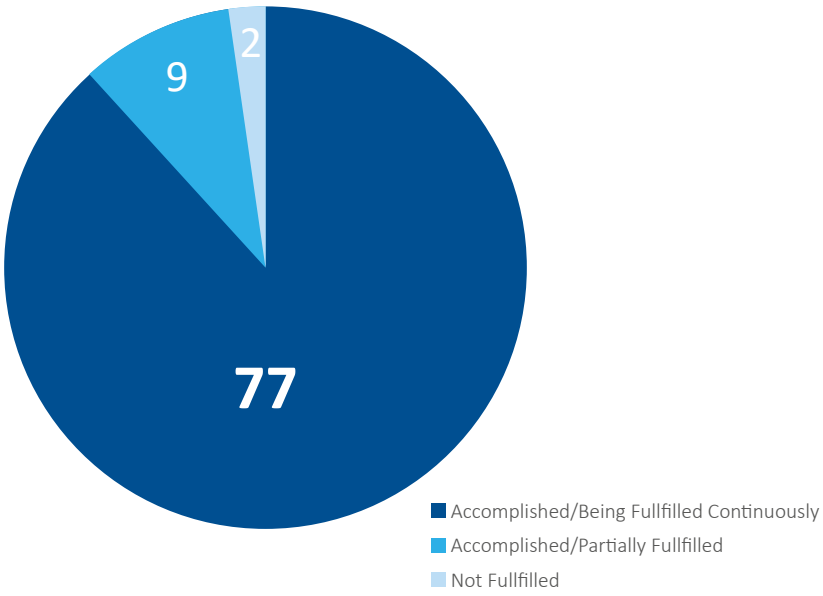
Through the working groups of the European Commission, the NÚKIB contributed to the structure and thematic focus of the Digital Europe Framework Programme, through which the European Commission allocates funds to the development of artificial intelligence, supercomputing, cybersecurity, and advanced digital skills

ANNEX 1: EVALUATION OF THE ACTION PLAN FOR THE NATIONAL CYBER SECURITY STRATEGY OF THE CZECH REPUBLIC FOR 2022

Year 2022 was the second year of evaluation of the Action Plan for the National Cyber Security Strategy of the Czech Republic for the period 2021 to 2025 (hereinafter referred to as the "Action Plan"). The NÚKIB not only coordinates the evaluation of the entire Action Plan, but also participates as a managing and co-operating entity in the implementation of 101 out of 105 tasks. In 2022, 88 tasks were subject to evaluation. 73 of these tasks are being completed continuously.

In 2022, 77 of the evaluated tasks were met or are being continuously reached. 9 tasks were met partially, and only 2 tasks were assessed as unfulfilled. Compared to 2021 (8 partially completed, 0 uncompleted tasks), this means a slight decrease in the success rate of the Action Plan. An example of a task scheduled and completed in 2022 is to *develop a methodological document on supplier security management and provide it to authorities and persons obligated under the Cybersecurity Act.* In consultation with the Ministry of Finance, the Ministry of the Interior, and the Ministry of Industry and Trade, the NÚKIB prepared a methodological document, which also took into account the supporting materials of the Ministry of Regional Development concerning public procurement. This resulted in a document dealing with the management of suppliers throughout the entire life cycle of the supply, taking into account the specifics of supplier relationships under Act No. 134/2016 Coll., on public procurement, as amended. In December 2022, the document was sent to relevant entities, and will be published on the NÚKIB website during 2023. On the other hand, an example of a task not yet completed was *the creation and organization of exercises in the field of cybersecurity for foreign partners of the Czech Republic in coordination and synergy with other Czech international activities.* Although the NÚKIB participated in international exercises in the field of cybersecurity in the past year, no specific exercises designed for foreign partners took place.

The main reason negatively influencing the implementation of the Action Plan were the Russian invasion of Ukraine and the resulting deterioration of the security situation, which depleted personnel and other capacities for more immediate and urgent tasks. The preparation and implementation of the historically second CZ PRES was the second factor, which, especially in the second half of the year, occupied a significant part of the staff capacity, especially in the area of international cooperation. An example of a task which was delayed due to CZ PRES was to *create an overview of the implementation of non-binding norms of responsible behaviour of states in cyberspace and actively participate in the promotion of their compliance, preventing their dilution and weakening, including in the area of respect for human rights among others.* Although cooperation with relevant institutions took place at the national level under the coordination of the Ministry of Foreign Affairs, a comprehensive overview of non-binding standards was not created by the end of the year. Partially fulfilled and unfulfilled tasks will continue to be worked on in 2023 so that they are fully completed.



Grapf 33: Evaluation of Action Plan Tasks for 2022

RESOURCES:

- Microsoft. 2022. Microsoft Digital Defense Report 2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

- Police of the Czech Republic. 2022. Development of registered crimes in 2022. https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx

- Czech Banking Association. 2022. The number of cyberattacks grows dramatically and they are still more sophisticated. ČBA launches the nation-wide education campaign #nePINdej!. https://cbaonline.cz/kybertest-2022

- NÚKIB 2022. Threats and vulnerabilities. https://www.nukib.cz/cs/infoservis/hrozby/#1

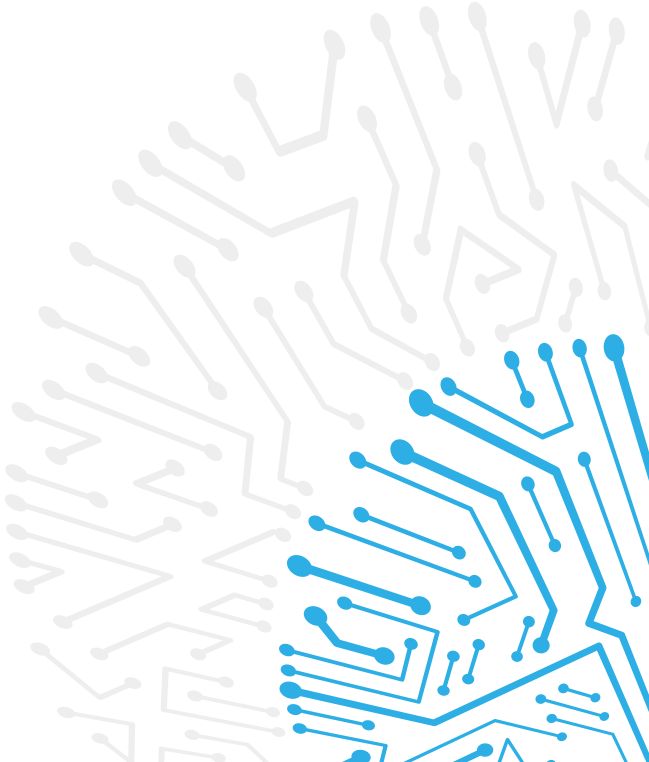
ABOUT THE NÚKIB

The NÚKIB is the central administrative body for cybersecurity, including the protection of classified information in information and communication systems and cryptographic protection. It is also responsible for the Galileo global navigation satellite system, a public regulated service. It was established on August 1, 2017 on the basis of Act No. 205/2017 Coll., amending Act No. 181/2014 Coll., on cybersecurity and on amendments to related acts (the Cybersecurity Act).

The NÚKIB currently helps ensure the cybersecurity of the Czech Republic and its residents through:

- Provision of timely, clear, and relevant information to subjects of critical information infrastructure, basic service operators, and public administration bodies;
- ensuring the security of classified information in information and communication systems, including cryptographic protection;
- preparation of national security standards, laws, and sub-legal norms in the field of cybersecurity;
- providing technical assistance and other services, such as security scans using penetration testing techniques or vulnerability scans;
- conducting operational response to cyber incidents using expertise and access to information for effective incident management;
- organization of trainings and cyber exercises at national and international level;
- cybersecurity trends analyses;
- providing methodological support, education, and awareness in topics related to the field of cybersecurity;
- conducting cybersecurity research and development;
- assessing cybersecurity risks and taking appropriate corrective and preventive measures;
- monitoring compliance with the requirements of the Cybersecurity Act by regulated persons;
- representation of the Czech Republic in the bodies of international organisations active in the cybersecurity sector;
- cooperation with the public, private, and academic sectors at national and international level.

For more information about the NÚKIB, visit our website www.nukib.cz or follow the news on Czech cybersecurity on our social networks Twitter, LinkedIn, Facebook or Instagram. Recordings of some events organized by the NÚKIB or attended by its representatives can be found at the NÚKIB YouTube channel.



NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost