# 2023 Report on the State of Cybersecurity in the Czech Republic

- Cybersecurity threats and actors
- Targets of cyberattacks
- National cybersecurity level
- Cybersecurity trends for 2024 and 2025

# Director's Foreword


It is my great pleasure to present the Report on the State of Cybersecurity in the Czech Republic for the past year. Let me also thank you for your continued interest in our nation's cybersecurity efforts.

The year 2023 was characterised by significant challenges in the cybersecurity landscape, dominated by rises in hacktivism and cybercrime. Hacktivism, previously a less prominent issue, has surged in the context of Russia's aggression towards Ukraine. Over the past two years, it has evolved into a more organized and sophisticated threat. Many hacktivist groups operate with direct support from certain states and operate in alignment with the geopolitical interests of their governments. Consequently, the Czech Republic has experienced a substantial increase in DDoS attacks, bringing the total number of incidents handled by our agency to a record 262.

Cybercriminal activity also intensified, with a notable increase in incidents reported by the Police of the Czech Republic. The professionalization of these cybercriminals, particularly in relation to phishing attacks, has become increasingly apparent. The use of artificial intelligence (AI) has enhanced their ability to manipulate victims effectively, a trend that shows no signs of slowing. In response, we have strengthened our awareness-raising initiatives in collaboration with our partners. Prevention remains the most effective defence against phishing.

The past year also highlights a persistent and troubling interest from actors associated with the Russian Federation and the People's Republic of China. These covert actors have targeted Czech strategic institutions, with at least four confirmed intrusion attempts in the past year, cyber espionage very likely being the goal.
A major concern revealed in our findings is the stagnation of cybersecurity budgets across many organisations in the Czech Republic. This challenge is compounded by a shortage of cybersecurity professionals, particularly within the public sector. The inability to attract, compensate, and retain these professionals under the current economic conditions threatens our nation's ability to combat cyber threats effectively. Raising public sector salaries to the level of the private sector may not be feasible, yet state institutions struggle to remain competitive and lack the necessary experts to meet their cybersecurity and IT needs, even with external contractors. If this trend continues, our ability to maintain a secure and resilient cyberspace will be severely compromised.

To address these issues and to move forward, we must act decisively. It is .imperative to close the increasing salary gap for IT and cybersecurity professionals in the public sector. A secure, resilient, innovative and competitive nation requires that we invest in the people who safeguard our digital infrastructure. I firmly believe that such investment will yield significant returns for our country.

**Ing. Lukáš Kintr**
Director of the National Cyber and Information Security Agency

In closing, I thank the 423 organizations that participated in our survey and contributed to the 2023 Report on the State of Cybersecurity. This represents an increase of more than 100 respondents from the previous year and has enhanced the accuracy and comprehensiveness of our report.

At NÚKIB, our mission is to fortify the security and resilience of the Czech Republic in cyberspace. I am proud of our collective efforts and the progress we are making together.

# Obsah

# About the Report

## Questionnaire Survey

At the beginning of 2024, NÚKIB distributed a survey with 63 questions to entities regulated by Act No. 181/2014, on Cybersecurity and on Amendments to Related Acts (the Cybersecurity Act), as amended, and to several other key institutions and organizations not regulated by the Cybersecurity Act. The questions covered a wide range of topics, including cyberattacks, cybersecurity costs, cybersecurity staffing, users, technology and existing processes. A total of 423 entities responded, with 339 being regulated and 84 unregulated. The information obtained from these responses was used to inform NÚKIB for the 2023 Report on the State of Cybersecurity in the Czech Republic (hereinafter „Report"). All data from the survey were anonymised.

## Evaluation process

Assessment of the state of cybersecurity in the Czech Republic is based on an analytical process that includes quantitative and qualitative evaluations of the data from the completed surveys, NÚKIB's findings, information from its partners and open-source information. NÚKIB does not independently verify the data provided by the respondents or validate the accuracy of their statements. The analytical conclusions in the Report assume that the survey responses are unbiased. Probabilistic expressions (see below) are used to express the analytical evaluation.

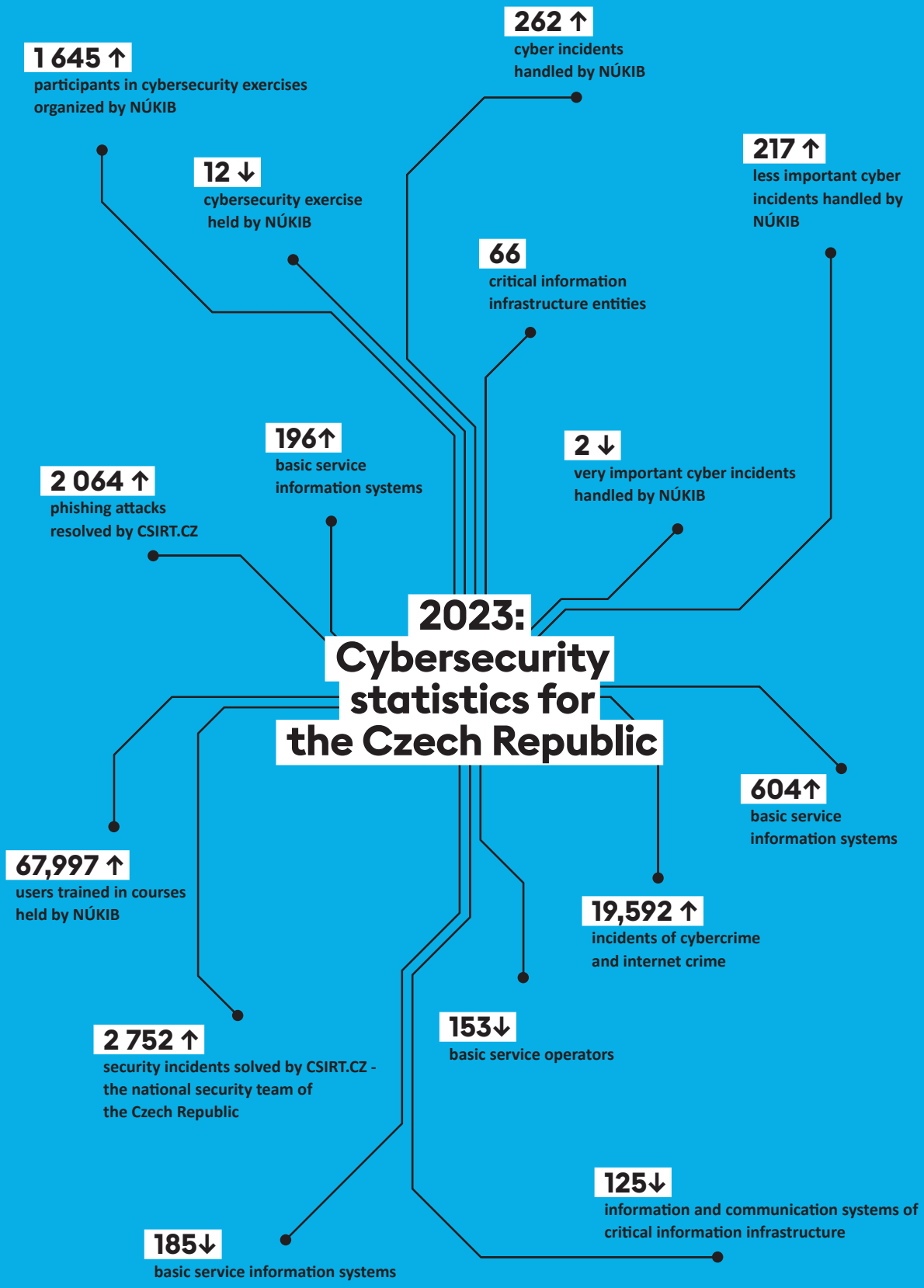
The Report does not provide a complete list of activities related to cybersecurity. Its purpose is to describe and evaluate the threats faced by the Czech Republic in cyberspace in 2023 and the activities that help mitigate these threats.

## Probabilistic expressions used in the 2023 Report on the State of Cybersecurity in the Czech Republic

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

# List of abbreviations

| | |
|---|---|
| AI | Artificial Intelligence |
| CERT | Computer Emergency Response Team |
| ČR | Czech Republic |
| CZ PRES | Czech Presidency of the Council of the European Union |
| DIA | Digital and Information Agency |
| DoS/DDoS | Denial of Service / Distributed Denial of Service |
| ENISA | European Union Agency for Cybersecurity |
| EU | European Union |
| GRU | Main Administration of the General Staff of the Armed Forces of the Russian Federation |
| LLM | Large Language Model |
| MPSV | Ministry of Labour and Social Affairs |
| NATO | North Atlantic Treaty Organization |
| NCTEKK | National Centre for Counter-Terrorism, Extremism and Cybercrime |
| NIS 2 | EU Directive on measures to ensure a common high level of cybersecurity in the Union |
| NÚKIB | National Cyber and Information Security Agency |
| PCSC | Prague Cyber Security Conference |
| PČR | Police of the Czech Republic |
| PRC | People's Republic of China |
| RGB | Reconnaissance General Bureau |
| SVR | External Intelligence Service |
| TTPs | Tactics, Techniques and Procedures |
| ZKB | Law on Cybersecurity |




*Visualization 1: Cybersecurity statistics for the Czech Republic*

# Summary of the Report on the State of Cybersecurity in the Czech Republic 2023

## 80% increase in the number of cyber incidents

In 2023, NÚKIB recorded an almost 80% increase in the number of cybersecurity incidents, rising from 146 last year to 262. This surge is mainly attributed to repeated waves of DDoS attacks by Russian-affiliated hacktivist groups and ransomware attacks targeting Czech strategic institutions or companies. Despite the overall increase, the number of significant cyber incidents decreased year-on-year.

## The most common types of cyberattacks and their context

**The most prevalent cyberattacks in 2023 included various forms of phishing (spear-phishing, vishing, quishing) and fraudulent CEO emails. DDoS attacks were primarily directed at the public and financial sectors. Many of the recorded incidents were linked to Russian aggression in Ukraine, and in a few cases, to the Israeli-Palestinian conflict.**

## Cyber espionage threats

NÚKIB detected at least four distinct threat actors attempting to or succeeding in penetrating the networks of Czech strategic institutions, with a high probability (75–85%) that cyber espionage was the objective.

## Work on legislation improvement and security measures

NÚKIB's notable activities in 2023 included the drafting of a new cybersecurity law, continuing the organisation's work to ensure a robust legislative framework for cybersecurity in the Czech Republic following the NIS 2 Directive published during the Czech Presidency of the Council of the European Union in 2022. The year 2023 was similar, marked by discussions, consultations with stakeholders and the public, and commencement of the formal legislative process.

## Project BIVOJ: Increasing the resilience of the Czech Republic

**In collaboration with partners, NÚKIB also advanced its work on the BIVOJ Project. The project aims to create a unified, secure shared platform that provides security and communication services for public sector institutions.**

## GOV.CZ

**One of the project's key results in 2023 was the migration of central state administrative bodies to a single gov.cz domain. This single domain will increase user-friendliness for citizens, improve legal certainty, and fortify resilience to DDoS attacks.**

## Awareness activities and cyber exercises

NÚKIB also continued its initiatives in raising cybersecurity awareness and organising cybersecurity exercises. This included collaboration on educational programmes for primary and secondary schools and raising the profile of cybersecurity within the retraining system. In 2023, the TELCO23 sectoral exercise for telecommunications service providers was held, and NÚKIB representatives participated in international cybersecurity exercises such as Locked Shields and Cyber Coalition.

## Looking ahead

**NÚKIB anticipates several key trends over the next two years: cyberattacks via the supply chain, geopolitically motivated cyberattacks, and the increasing impact of artificial intelligence on cybersecurity.**

# 1 Cybersecurity in the Czech Republic in 2023 from the perspective of NÚKIB[1]

[1] The information presented in this document is based on NÚKIB sources and an evaluation of 423 survey responses (see section “About the Report”).

**In 2023, NÚKIB registered a total of 262 cybersecurity incidents, the highest number to date.**

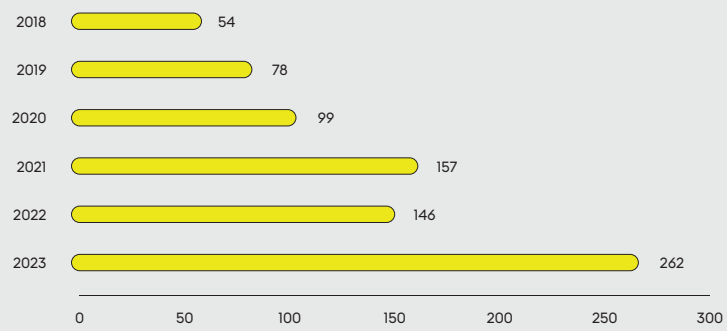
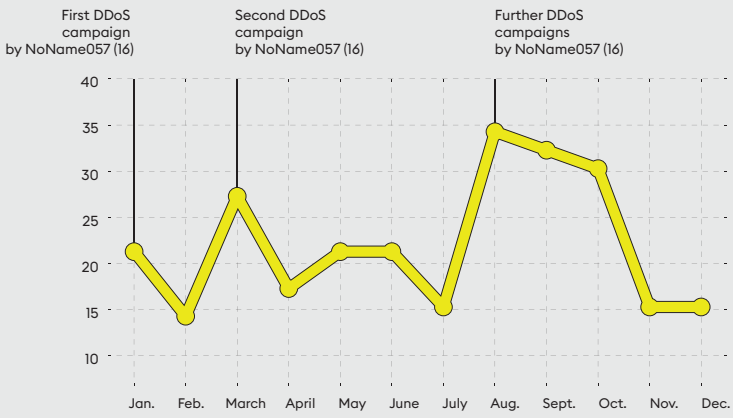



*Figure 1: Evolution of the number of incidents registered by NÚKIB in 2018–2023*

This marks an increase of nearly 80 % compared to 146 incidents registered in 2022.

This increase was driven primarily by repeated waves of DDoS attacks, led mostly by Russian-affiliated hacktivist groups.

**DDoS attacks accounted for a significant portion of all incidents in 2023. The group NoName057(16) was identified as the most frequent perpetrator of these attacks, which regularly targeted Czech entities.**




**262 incidents in total**

*Figure 2: Evolution of the number of incidents registered by NÚKIB in 2023*

The NoName057(16) campaigns against Czech targets typically coincided with events or statements linked to the conflict in Ukraine or other major occurrences. Examples include attacks in response to announcements of material or other assistance to Kyiv, or statements by Czech political leaders regarding the conflict in Ukraine. The Czech Republic was among the European countries most often targeted by this actor (Fig. 3).

**However, the impact of the reported attacks was not severe and resulted, in most cases, in temporary unavailability of the targeted entities' websites. DDoS attacks generally disrupt traffic on websites and services accessible from the internet without compromising the internal information systems of organisations.**

## Number of declared DDoS attacks on European countries by NoName057(16) in 2023

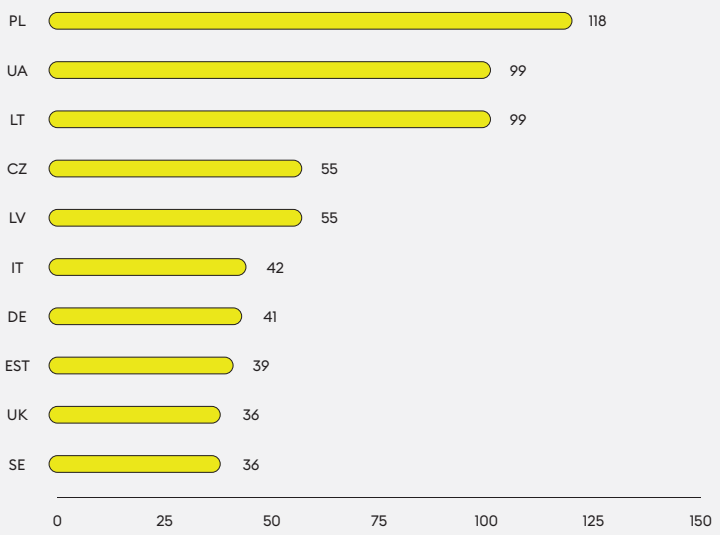



*Figure 3*

In 2023, NÚKIB also recorded several DDoS attacks in which the attacker could not be identified.

One such example was the DNS NXDOMAIN campaign, its name based on the flooding attack technique it used. This campaign was notable for its lack of correlation with geopolitical events or the activities of the targeted organisations, leaving the motives behind the attacks unclear. Alongside the techniques and infrastructure used in this campaign, the only clues were the specific victim profile, as these attacks exclusively targeted Czech state institutions.

**Ransomware attacks have been consistently recorded by NÚKIB since 2018. In June 2023 however, NÚKIB observed a noticeable increase in ransomware activities targeting strategically important Czech entities, prompting NÚKIB to issue an alert about the heightened risk.** The most prominent actors in the statistics were the PLAY and LockBit gangs, mirroring global trends. Apart from those, NÚKIB registered numerous phishing campaigns carried out by both state-sponsored actors and cyber-criminal groups.

In June 2023 NÚKIB observed a noticeable increase in ransomware activities targeting strategically important Czech entities

## While less important incidents more than tripled, important incidents decreased by a third.

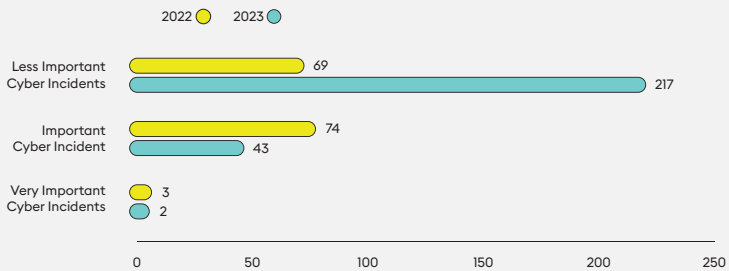


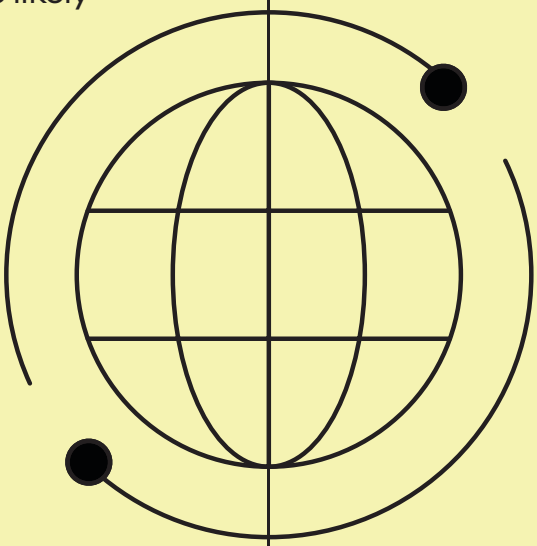

*Figure 4: Evolution of the number of incidents registered by NÚKIB in 2022–2023*

In terms of the severity of the incidents registered, positive developments were observed, with a year-on-year decrease in the number of important and very important cyber incidents despite a significant increase in the overall number of incidents (Fig. 4). The increase in the number and reduction of severity of registered incidents can be attributed to the repeated DDoS attacks against Czech targets, which are prominent in NÚKIB's statistics but generally had no significant or long-term impacts.

**In the short-term outlook for the next three years, several emerging trends are expected to persist.**

### Cyberattacks in connection with geopolitical events

Cyberattacks in response to geopolitical events or other politically sensitive events, not necessarily limited to the context of the conflict in Ukraine, are likely (55–70 %) to continue.



### Involvement of hacktivist groups

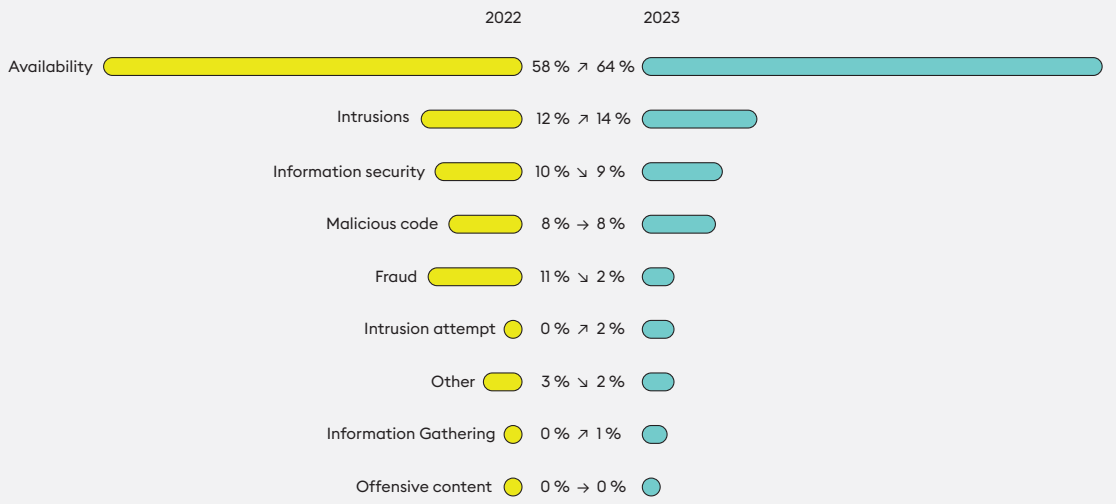
The involvement of various hacktivist groups is expected, but other types of actors cannot be ruled out (25–50 %).

### Phishing campaigns and ransomware attacks

It is also highly likely (75–85 %) that broad phishing campaigns against both national authorities and private entities will continue, along with ransomware attacks across multiple sectors.

# Classification of cyber incidents reported to NÚKIB[2]

## Percentage of representation in incidents




**Availability** - Availability disruption caused by DoS/DDoS attacks or sabotage
**Intrusions** - Compromising of applications or user accounts
**Information security** - Unauthorized data access, unauthorized data modification
**Malicious code** - Viruses, worms, Trojan horses, dialers or spyware
**Fraud** - Phishing, identity theft or ICT unauthorized use
**Intrusion attempt** - Vulnerability exploitation attempts, login attempts etc.
**Information Gathering** - Scanning, sniffing, social engineering

*Visualization 2: Classification of cyber incidents reported to NÚKIB*

**In terms of incident classification, incidents targeting the availability of websites or services were dominant in relation to the high number of observed DDoS attacks.** This category also includes incidents caused by technical errors leading to system failures.[3]

**The second largest category was intrusions,** mainly consisting of social engineering attacks, most often in the form of phishing, leading to the compromise of email or other accounts. **The third most frequently recorded incident category was information security, ransomware attacks being prevalent.**

---

2 Classification of cyber incidents is based on ENISA taxonomy: Reference Incident Classification Taxonomy – ENISA (europa.eu)

3 Under the provisions of the current Act on Cybersecurity, regulated entities are required to report all cyber incidents, i.e., information breaches in information systems, security breaches in services or security breaches in the integrity of electronic communications networks due to a cybersecurity incident.

# Incidents as seen by entities

## Increasing phishing frequency and sophistication

**From the perspective of the surveyed companies, phishing has long dominated cyberattack statistics.**

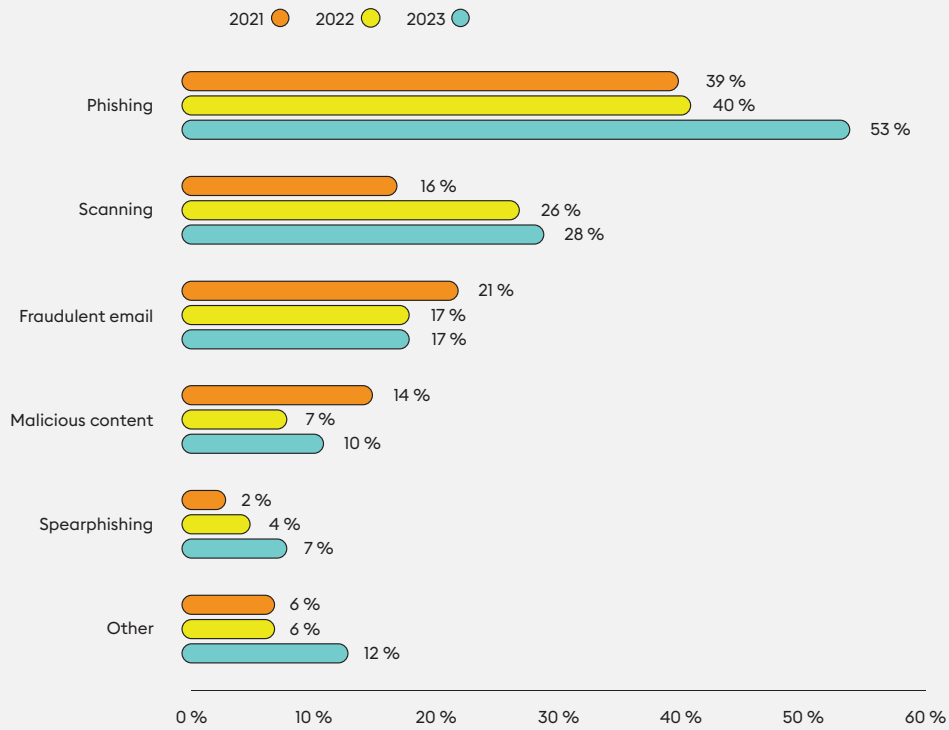



*Figure 5: Most common cyberattack categories in 2021–2023 (% of respondents)*

**However, 2023 data indicate a significant rise in the use of this technique,** with more than half of respondents identifying phishing as the most frequent type of attack (Fig. 5). **An increase is also evident in the category of targeted spear-phishing attacks, aligning with the trend of increasing phishing frequency and sophistication observed by NÚKIB.**

# Total incidents steady at previous year's level

Year-on-year, the number of cyberattack attempts resulting in a cyber incident remained largely unchanged (Fig. 6); the proportion of successful cyberattack attempts resulting in a cyber incident was also steady (Fig. 7).

**Number of attempted cyber-attacks that triggered an incident in 2023 (% of respondents)**

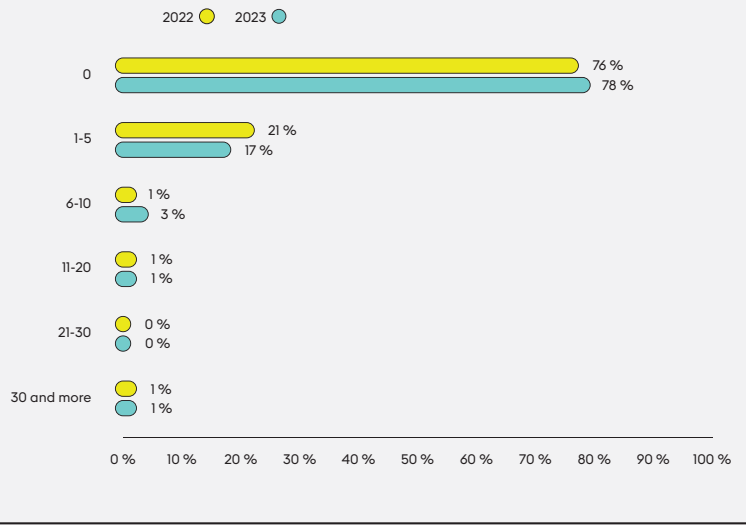



*Figure 6*

**Comparison of recorded or attempted cyberattacks in 2022 and 2023 (% of respondents)**

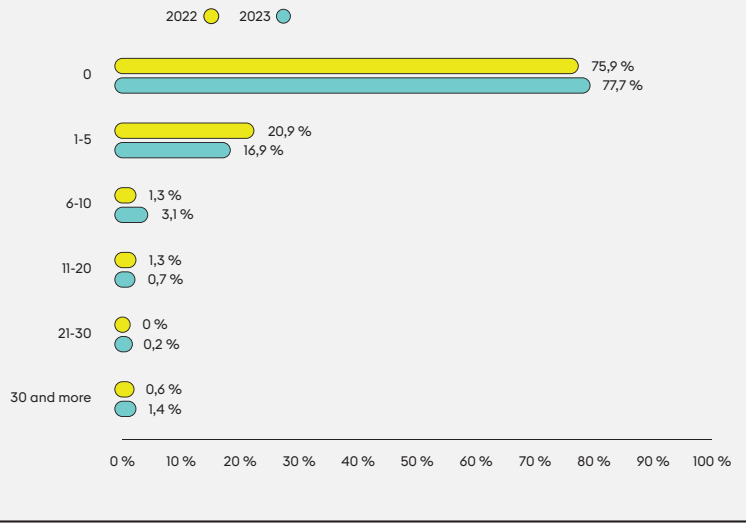



*Figure 7*

This suggests that improvements in attackers' techniques have not significantly impacted the cybersecurity of entities.

# Cybersecurity budgeting: Stagnating organisational cybersecurity budgets

**Over the past two years, budgets allocated to the cybersecurity of individual organisations have stagnated.** Of the surveyed organisations, 47 % reported budget increases, representing a 3 % year-on-year growth. However, taking into account the high inflation over the past two years, budget increases are probably in comparison to nominal amounts. These increases therefore likely (55–70 %) match inflationary pressures and price hikes, with more than half of respondents reporting no real budget increases.

**The proportion of organisations that consider their cybersecurity budget sufficient has remained nearly unchanged year-on-year (Fig. 8).** Over half of respondents still regard their cybersecurity spending as insufficient.

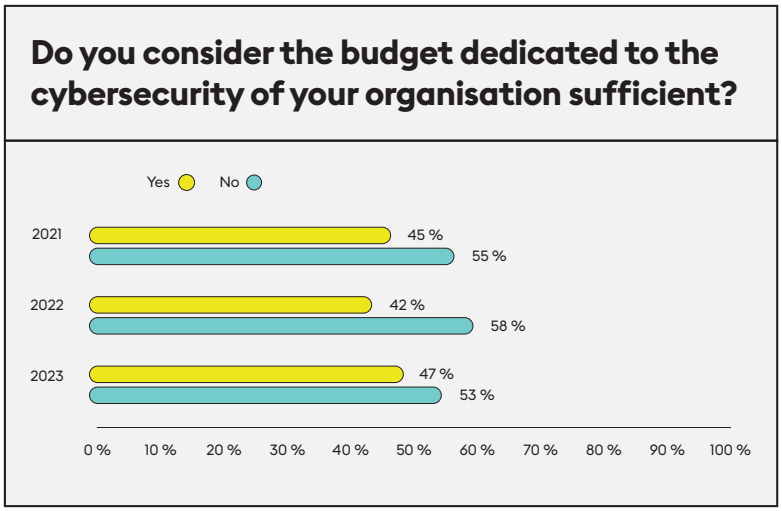



*Figure 8*

Three quarters of organisations dedicate 0–5 % of their budget to cybersecurity (Fig. 9), comparable to last year's results for the portion of total budget dedicated to cybersecurity.

Looking ahead, 55 % of respondents indicate plans to increase cybersecurity budgets, suggesting that the trend of stagnation may turn into slight budgetary increases depending on economic conditions.

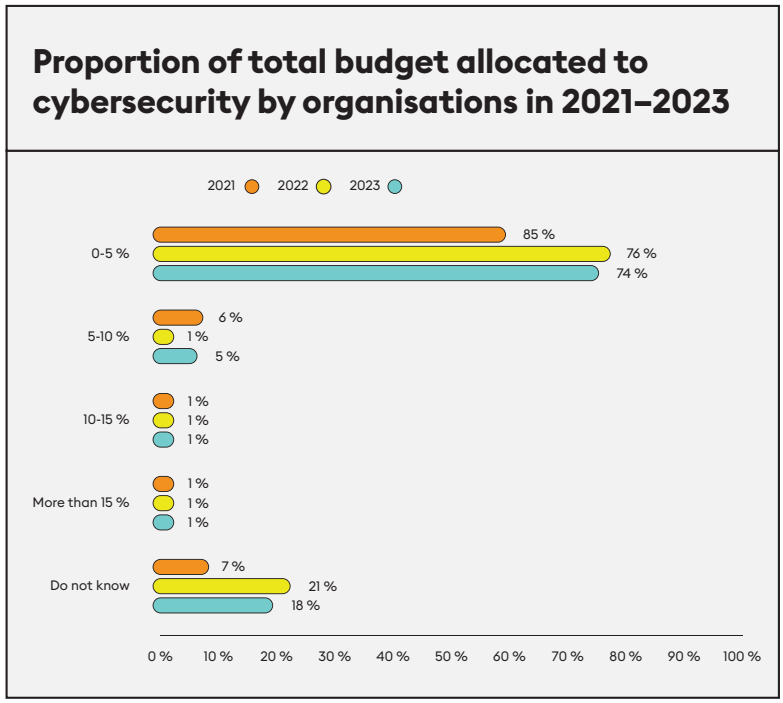



*Figure 9*

# Workforce challenges: Shortage of cybersecurity experts

**The shortage of cybersecurity experts remains a significant challenge for Czech institutions and organisations.** Insufficient renumeration in the public sector is a persistent problem, with **more than half (54 %) of respondents citing salary requirements as the most critical factor discouraging candidates.**

Organisations address this issue in various ways, with ongoing trends emerging over the last three years (Fig. 10).

## How organisations addressed their shortage of experts in 2020–2023 (% of respondents)

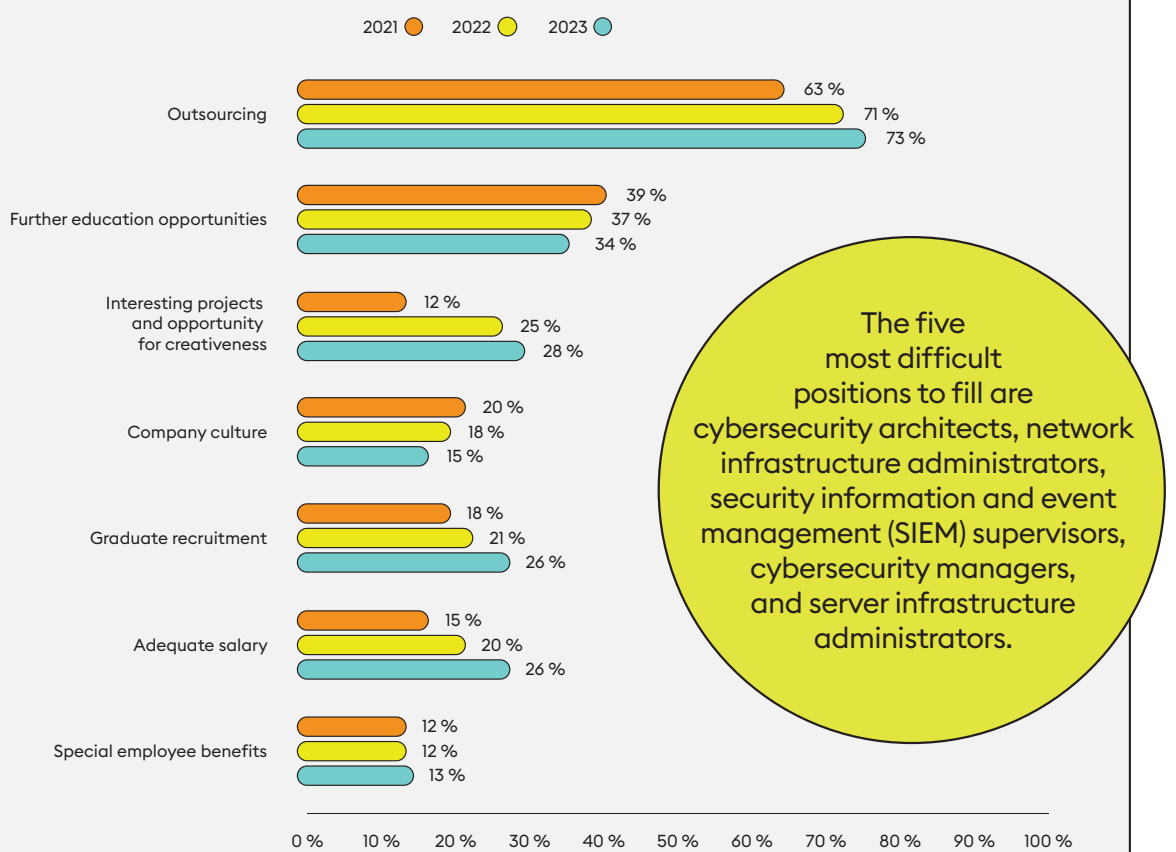



*Figure 10*

For example, the proportion of organisations outsourcing cybersecurity experts to address their shortages has seen steady growth since 2020, although the growth rate of this approach is slowing.

Further training to address shortages, despite remaining the second most common solution, is decreasing, with a steady decline observed since 2020. Recruitment of graduates has steadily increased by 8 % over the last three years.

Adequate renumeration category has also risen by 10 % over the same period, **but in more than half of cases, respondents cited low salaries as the primary factor complicating the filling of key positions (Fig. 11).**

## Key factors seen by respondents as discouraging candidates from recruiting to cybersecurity posts (% of respondents)

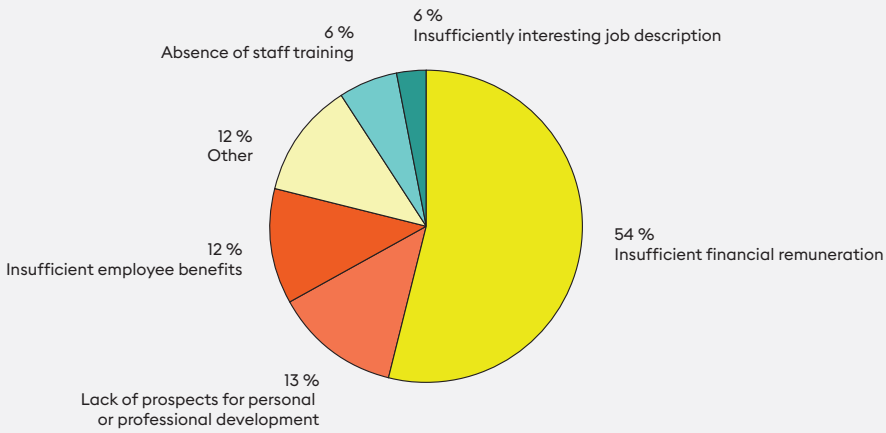
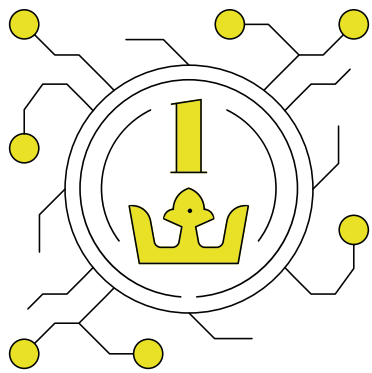



*Figure 11*

More than half (54 %) of respondents citing salary requirements as the most critical factor discouraging candidates.

The five most difficult positions to fill are cybersecurity architects, network infrastructure administrators, security information and event management (SIEM) supervisors, cybersecurity managers, and server infrastructure administrators.



# Workforce training: Positive shift in cyber resilience testing

**Proportion of organisations training/not training their employees in cybersecurity (% of respondents)**

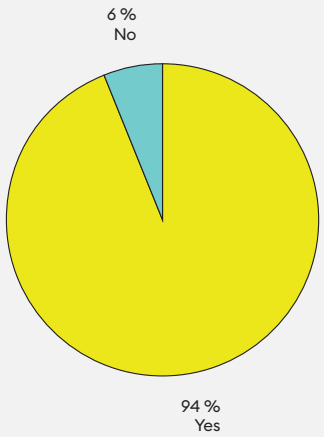


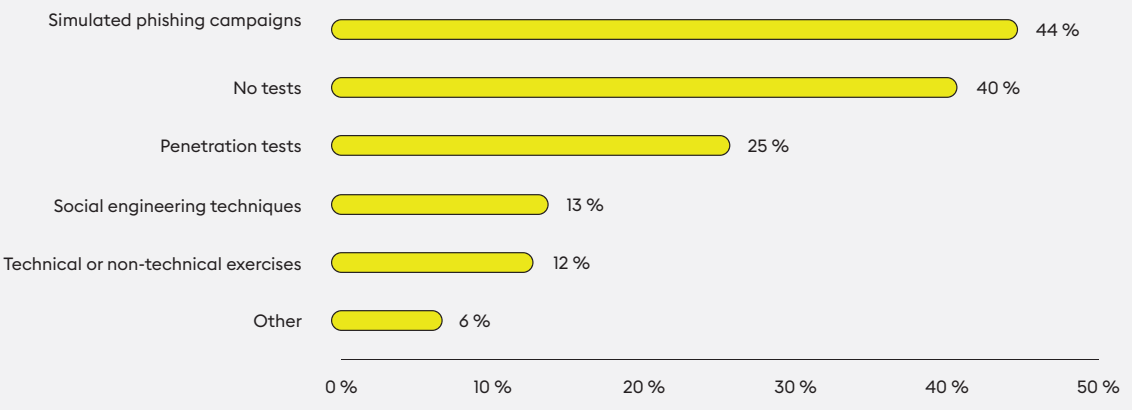

*Figure 12*

Across all sectors, most surveyed organisations train their staff in cybersecurity or familiarise them with current cyber threats at least once a year. Only 6 % of respondents do not train their employees at all (Fig. 12).

Informing staff via email or internal portals is the most widespread training method, used by almost two thirds of the respondents.

Organisations in the healthcare and education sectors provide the least training, with around 85 % of the surveyed organisations offering training.

**Methods of testing staff resilience to cyber threats in 2023 (% of respondents).**

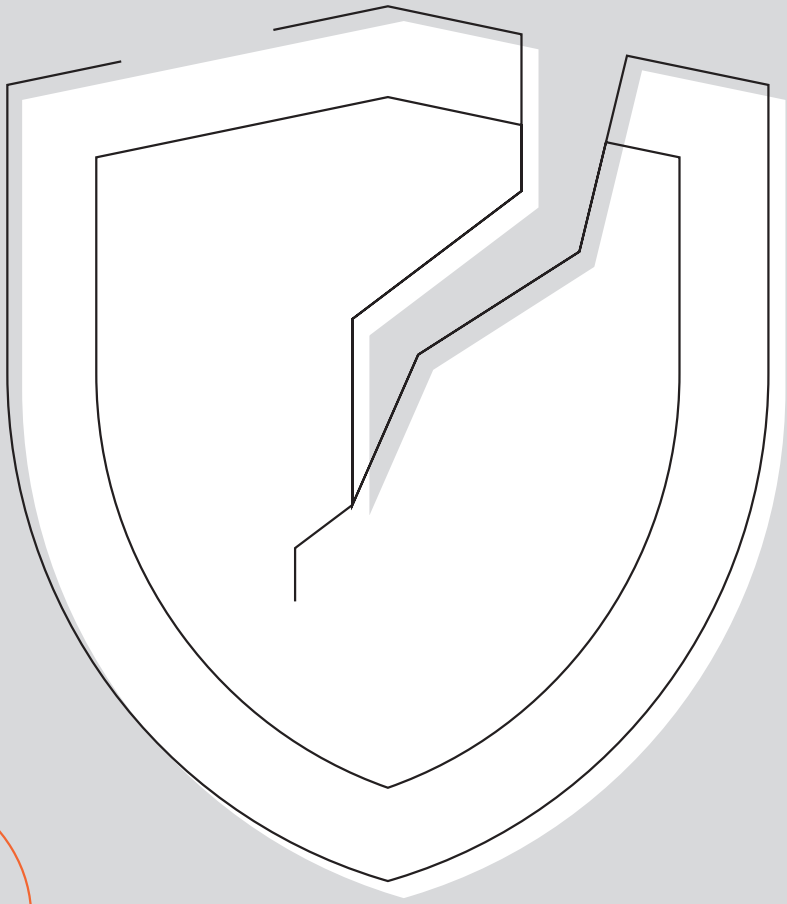



Simulated phishing campaigns are the most common form of testing

However, 40 % of organisations do not conduct any testing of their staff.

*Figure 13*

# Cybersecurity threats and actors



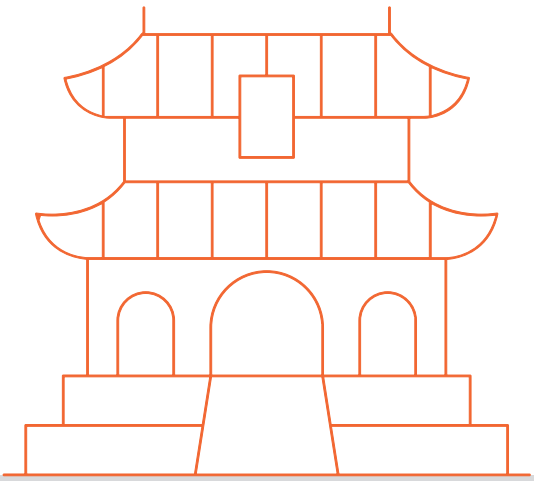
2

# Russian and Chinese actors have consistently attempted to penetrate the networks of strategic institutions in the Czech Republic.

NÚKIB, in collaboration with its partners, has identified intrusion attempts or successful intrusions by at least four distinct threat actors targeting the networks of strategic institutions. Analysis of victim profiles and TTPs in all cases suggests a high likelihood (75–85%) that the objective was cyber espionage.

In the face of state-sponsored threats, the Czech Republic confronts similar challenges to its EU and NATO allies.

**Threat actors primarily seek to establish long-term presence (persistence) in targeted networks, especially within strategic institutions.** This is in line with their tactics, techniques, and procedures (TTPs), with cyber espionage as their primary objective.



## Russian activities associated with APT29 and APT28

Activities associated with the Russian Federation were almost certainly (90–100 %) part of long-standing campaigns also affecting allies. **These malicious activities have tradecraft, motivation and objectives that overlap significantly with APT29 (known as Midnight Blizzard, BlueBravo and Cozy Bear) and APT28 (known as Forest Blizzard, BlueDelta and Fancy Bear).** The first of the above-mentioned actors is associated with Russia's foreign intelligence service (SVR) and the second with Russian military intelligence (GRU).[4]

## Increased activity of PRC-related actors

Over the past several years, NÚKIB has also detected increased activity from actors associated with the People's Republic of China (PRC), driven by their heightened focus on European objectives in the context of the war in Ukraine. **In 2023, an intrusion into a strategic institution's network was highly likely (75–85 %) perpetrated by a Chinese-origin attacker.** Mustang Panda's phishing campaign (known as RedDelta) has directed significant effort against European objectives, including those in the Czech Republic, at least since the beginning of Russia's invasion of Ukraine.

## North Korean interest in the defence sector

The Czech Republic was targeted by the North Korean group Lazarus (known as Diamond Sleet or Labyrinth Chollima) in 2023. **The group's objective was to compromise defence companies in the Czech Republic and other NATO/EU countries.** The group is associated with the Reconnaissance General Bureau (RGB).[5] and **their campaign verifies the interest of selected threat actors in specific sectors of the Czech industry.**

## Lower activity of Iran

In the context of the escalation of the Israeli-Palestinian conflict, activities by Iranian actors targeting the technologies of specific producers in the water sector have been detected. However, the activity of sophisticated actors operating in line with Tehran's interests was lower than in the past.

---

[4] See, for example: SVR cyber actors adapt tactics for initial cloud access - NCSC.GOV.UK / BlueBravo Adapts to Target Diplomatic Entities with GraphicalProton Malware | Recorded Future / Office of Public Affairs | Justice Department Conducts Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate of the General Staff (GRU) | United States Department of Justice / Vojenské zpravodajství | Tiskové zprávy - Vojenské zpravodajství provedlo aktivní zásah v kybernetickém prostoru (vzcr.cz)

[5] See, for example: Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups | U.S. Department of the Treasury / Not So Lazarus: Mapping DPRK Cyber Threat Groups to Government Organizations | Mandiant

# **Ransomware:** Innovations in extortion tactics

Ransomware attacks continue to evolve, with attackers developing new tactics and techniques to increase the likelihood of harvesting ransoms.

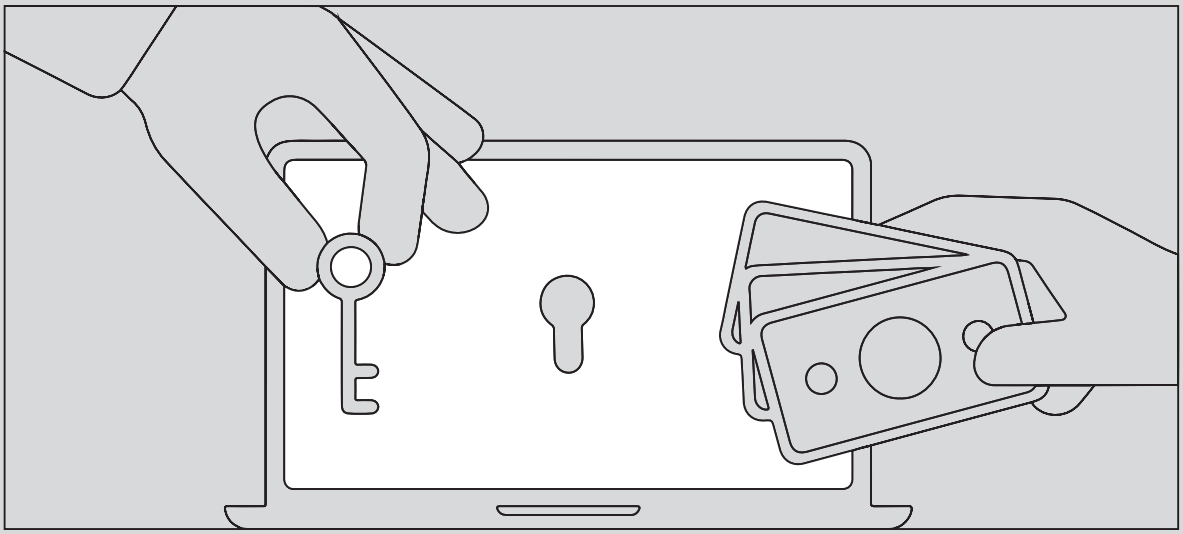
**In 2023, NÚKIB observed the first case of an extortion-only ransomware attack, where attacker exfiltrated the victim's data and threatened to publish it unless a ransom was paid.**

This tactic is an evolution of the already established tactics of double or multiple extortion strategies. The ransomware-as-a-service model also remains prevalent.

It is highly likely (75–85 %) that attackers will continue to develop innovative methods to coerce their targets into paying ransoms.

**However, payment of a ransom never guarantees the resolution of the incident or restoration of data, and it provides attackers with resources to carry out further malicious activities.**

Efforts to discourage the payment of ransoms have culminated in a statement by the International Counter Ransomware Initiative pledging to refrain from paying ransoms–a commitment that the Czech Republic has also joined.



# Phishing: Increasing frequency and sophistication

**In its various forms, phishing has long been the most widespread attacker technique.** The majority of survey respondents encountered this threat in 2023 (Fig. 14). **More recent forms of phishing, including vishing, smishing and quishing, were frequently mentioned.**

**Distinct phishing types encountered by respondents in 2023 (% of respondents)**

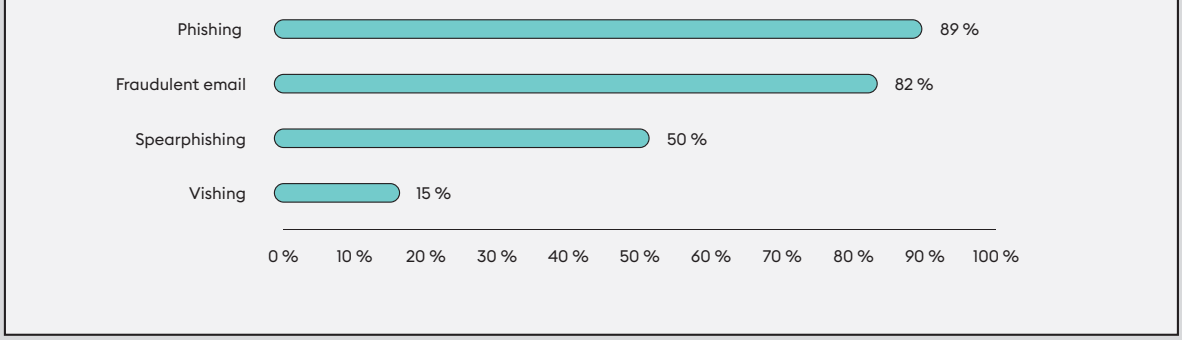



*Figure 14*

CEO email fraud, where attackers impersonate an organisation's director to authorise fund transfers, was also identified as a significant threat in 2023.

**NÚKIB itself was impersonated in a vishing campaign (see section "Financial Sector").**

The quality of all types of phishing attacks continues to improve, often appearing more credible and grammatically correct, sometimes displaying detailed knowledge of the victim or organisation.

**This increase in quality is likely (55–70 %) due to the availability of AI tools and the proliferation of specific phishing tools on the dark web** (see section "Cybersecurity trends in the Czech Republic for 2024 and 2025").

# Phishing

**Fraudulent action by attackers attempting to obtain sensitive information from their victims or to induce them to take a specific action**

### Vishing

Uses telephone or internet calls, which can mimic the numbers of real organisations (spoofing), the names of their representatives or even cloning their voice via AI

### Smishing

Uses SMS messages, often impersonating different institutions such as banks, transport companies, etc.

### Spear-phishing

Uses detailed knowledge of the victim or the environment in which the victim works or lives

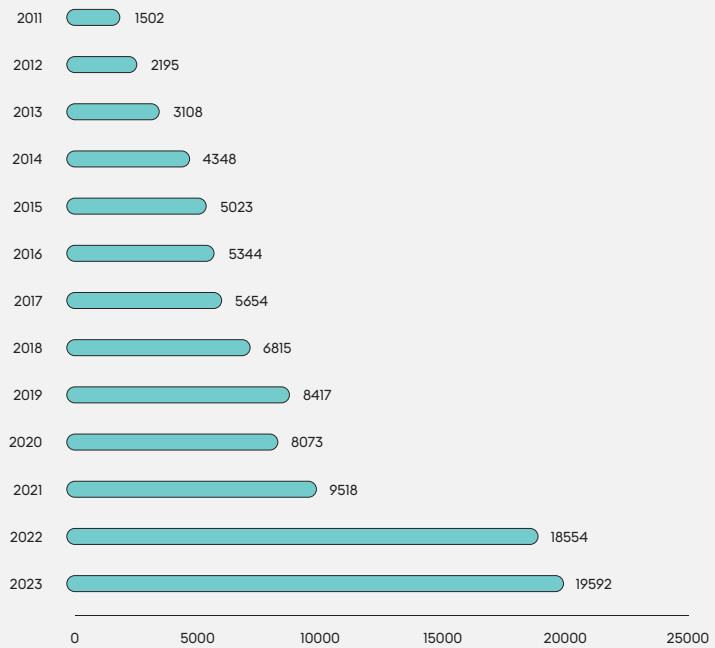
### Quishing

This relatively new technique misuses QR codes to spread harmful links. There have been observed cases of dissemination, e.g. through business cards at social events

*Visualization 3: The different types of phishing*

# Evolution of cybercrime in the Czech Republic since 2011

**According to data from the Police of the Czech Republic (PČR), 19,592 criminal offences were committed in cyberspace in the Czech Republic in 2023, representing a 6 % year-on-year increase**




**2022 saw a significant increase, with cybercrime activities nearly doubling year-on-year.**

*Figure 15 : Evolution of criminal offences in cyberspace registered by the Police of the Czech Republic in 2011–2023*

From 2011 to 2021, cybercrime exhibited a gradual upward trend. By 2022, cybercrime accounted for more than 10% of total registered crime, up from 0.5% in 2011 and 5% in 2020 (out of a total 181,991 acts). The upward trend continued in 2023, but the increase has stabilised, returning to gradual year-on-year growth.

**PČR attributes this stabilisation to multiple prevention activities, which have raised awareness of the most common forms of crime committed in cyberspace** among potential victims and reduced their engagement in certain risky forms of electronic communication, such as selling second-hand goods on internet marketplaces.

PČR attributes the stabilisation to multiple prevention activities, which have raised awareness of the most common forms of crime committed in cyberspace.

# Police statistics on cybercrime are divided into:

## Comments by the PČR

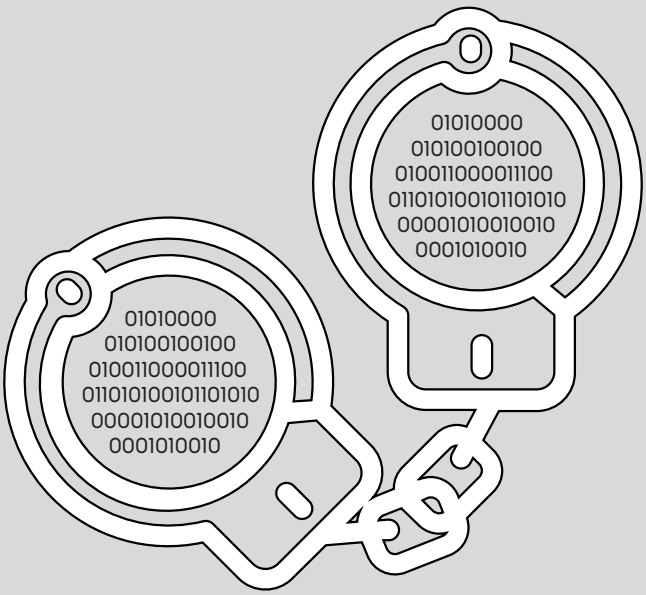
Since 2011, police statistics have covered two distinct areas of crime committed in cyberspace, as defined by the PČR in 2020.

**Cybercrime**

This category includes crime targeting information and communication technologies and the data they contain. Commonly referred to as 'hacking' and committed by 'hackers', these activities present a long-term, significant technological challenge and pose a threat to both civil society and national security. This type of crime is termed 'cyber-dependent crime'.

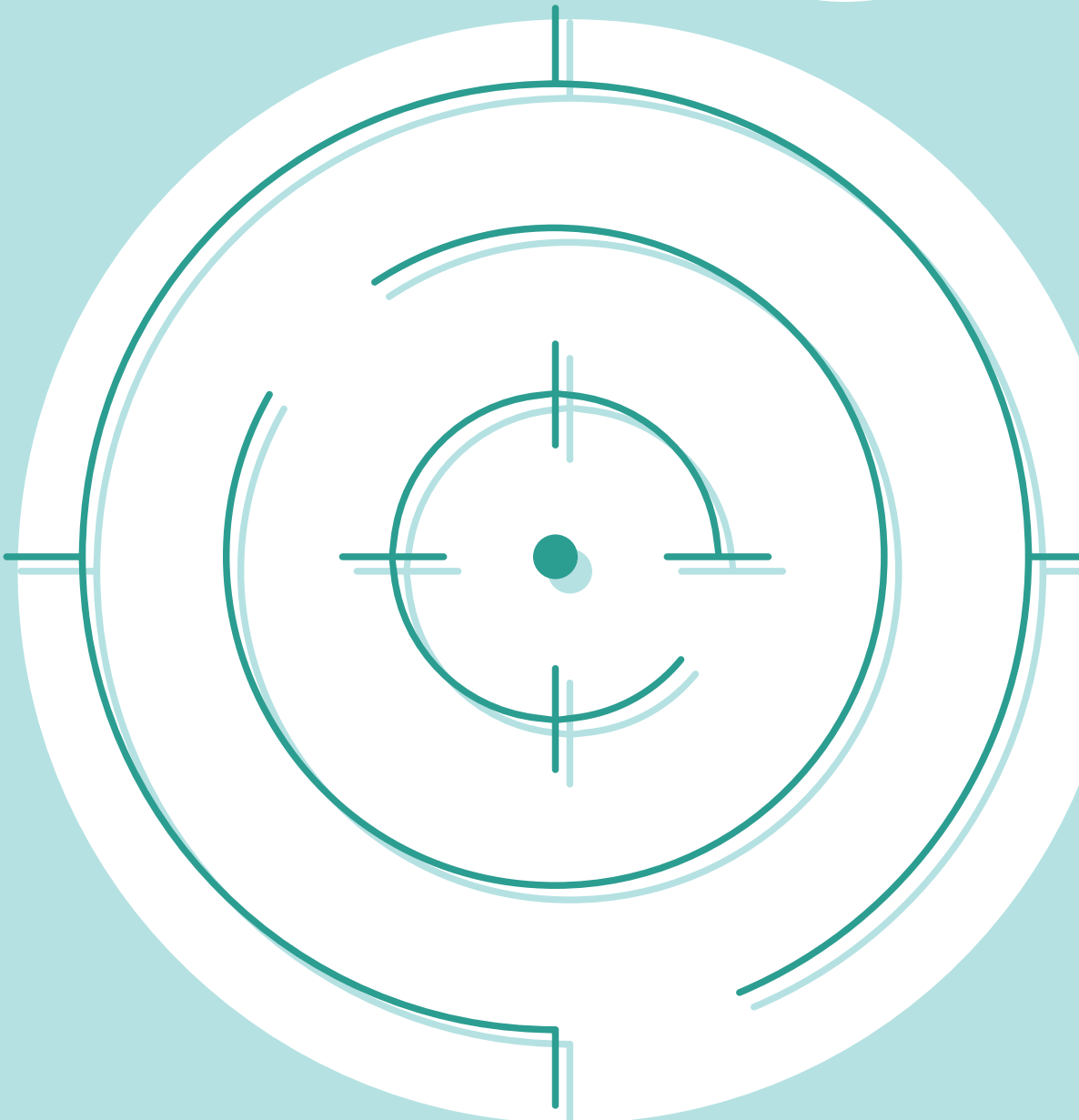
**Other crime committed in cyberspace**

In simplest terms, this category includes general and economic crimes such as fraud, extortion, hate speech, sexual abuse and drug distribution, for which information and communication technologies (computers or mobile phones) are merely tools for committing these crimes. This category can also encompass complex criminal activities, particularly those targeting large numbers of victims or significant entities, and often involves the use of modern, anonymous communication methods.



# Sectors targeted by cyberattacks

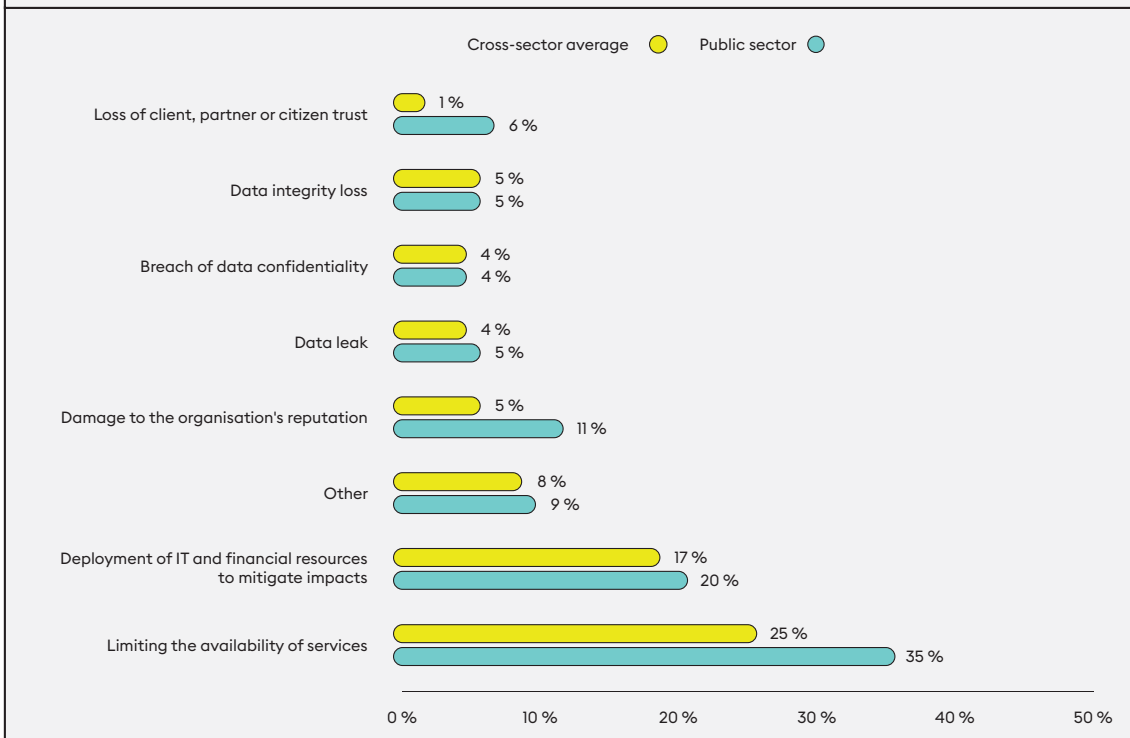
3



# Public sector: Focus on data and service availability

The public sector remains highly exposed to cyberattacks, with a notable increase in both attack attempts and cyber incidents in 2023. Despite this rise, the severity of these incidents decreased year-on-year, resulting in a lower overall impact.

**Impact of cyber incidents, comparison of public sector respondent testimonies vs. average (% of respondents)**




**The majority of cyberattacks targeted data availability, particularly though DDoS campaigns directed at Czech government and public institutions**

*Figure 16*

Compared to last year, the degree to which they could be directly linked to specific actions taken by the Czech Republic in support of Ukraine has decreased, but most of these campaigns were still attributable to Russian-affiliated actors. As in the previous year, these attacks were less sophisticated and had a limited impact

The public sector has long struggled with a lack of funding for cyber security. More than half of respondents rate the funding allocated to cybersecurity as insufficient.

**Is your organisation planning to increase its cybersecurity budget for next year? Comparison of public sector vs. average (% of respondents)**

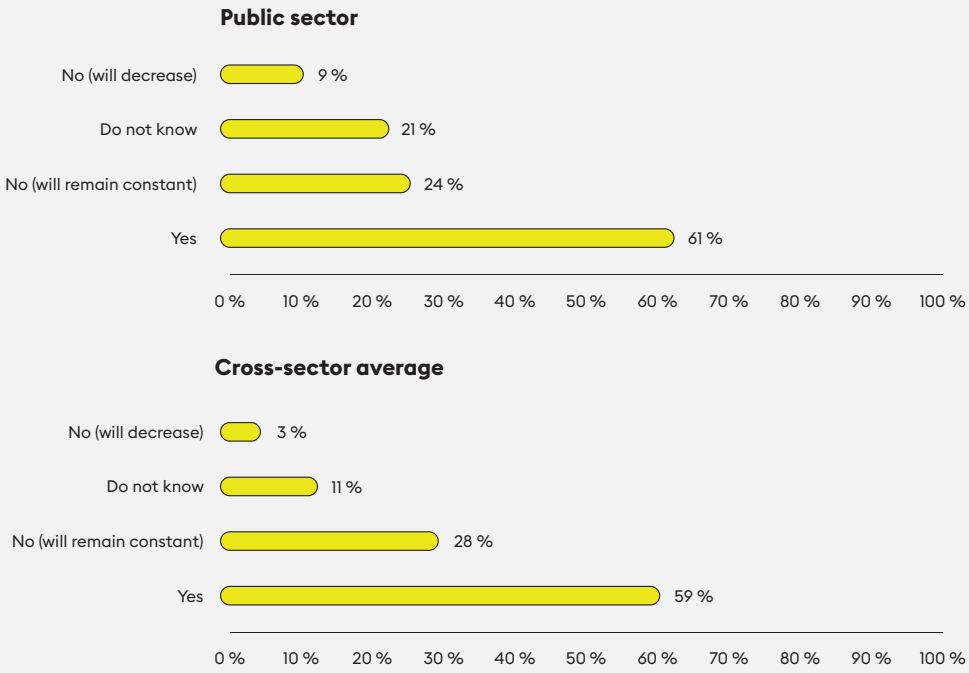



*Figure 17*

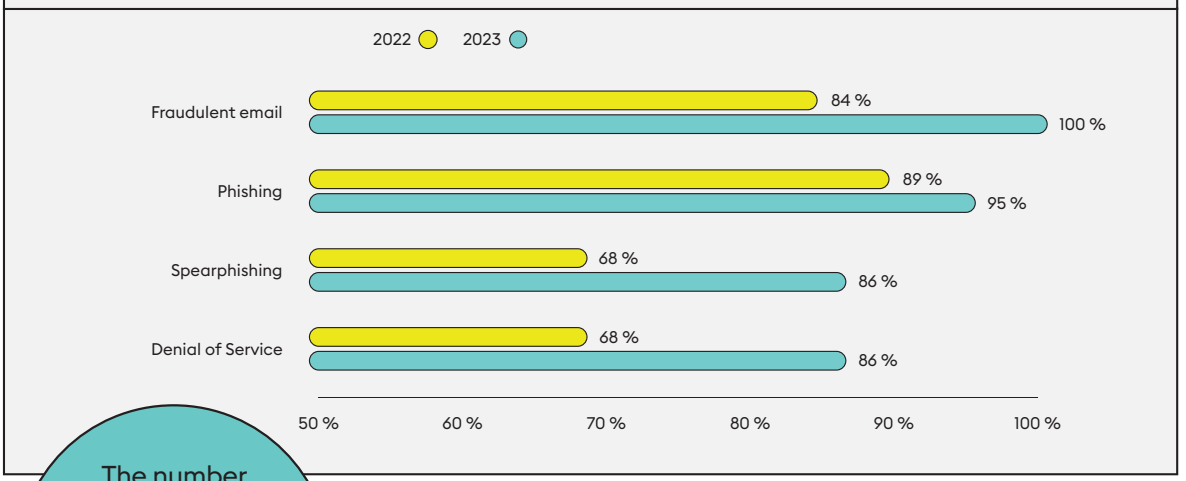
A look at the expected cybersecurity budget for public institutions shows that six percent more respondents than the national average indicate a decrease in the budget (Fig. 17). A minor positive may be that a majority of respondents expect it to increase, even two percent more than the average for other sectors. However, it is still the case that this increase may simply be an attempt to offset inflationary pressures.

The main factor negatively affecting the budget level was very likely (75-85%) the government's consolidation package, which, among other things reduces the funds available to the public sector.

# Financial sector: Attacks on banking service availability and advanced fraud targeting banking clients

The financial sector, like the public sector, has experienced a rise in DDoS attacks conducted by Russian-affiliated hacktivists over the past year. For the financial sector, particularly banks, this was a new trend linked to the conflict in Ukraine.

**Number of financial sector respondents who reported different forms of phishing or availability attacks (% of respondents)**




The number of respondents who experienced DDoS attacks in 2023 increased by nearly 20 %

*Figure 18*

Nearly two thirds of respondents from the financial sector reported that these attacks impacted the availability of services, **particularly affecting banking apps and websites, although disruptions generally lasted no more than an hour. Approximately half of the entities reported a DDoS attack as the most serious incident of the year.**

## Fraudulent phone call campaign impersonating NÚKIB and others

In August 2023, a fraudulent campaign was brought to NÚKIB's attention involving the impersonation of NÚKIB and several banking institutions. Attackers either directly impersonated NÚKIB employees, spoofing their phone numbers, or posed as banking institution employees referring to NÚKIB staff. In both cases, fraudsters pressured victims using various threats to transfer money from their bank accounts to a 'reserve back-up account', claiming the transaction was supervised by NÚKIB. To increase their credibility, the attackers used the names of actual NÚKIB staff obtained from publicly available sources. They exploited the fact that these names could be verified to support their deceptive claims by calling NÚKIB or searching publicly available information.

Various forms of phishing and fraudulent emails pose another ongoing threat to the financial sector. **This threat affects both the organisations' employees and their clients, with many respondents confirming an increase in the volume and sophistication of phishing attacks designed to extract funds from victims.**

# Industry and Energy:
# Sophisticated phishing techniques likely using AI tools

Energy is an extremely critical sector due to its high number of dependent services. The likelihood of the energy sector being targeted increased in 2023 as a result of the ongoing conflict in Ukraine and the European Union's efforts to shift towards importing energy products from other markets (e.g., Norway, USA, Azerbaijan, and Persian Gulf countries). The Czech water sector also faced cyberattacks last year following escalation of the Israeli-Palestinian conflict.

In 2023, 63 % of the surveyed organisations from the energy and industrial sectors faced attempted cyberattacks.

## Pro-Iranian actor targeted entities that use Unitronics devices

Over the past year, several entities in the water sector were targeted by a pro-Iranian group as part of a global campaign against users of devices produced by the Israeli company Unitronics. **Although operation of these devices has not been significantly compromised, the attacks illustrate how Czech entities can be affected by international conflicts.**

**The energy and industrial sectors also differ from other sectors in their level of satisfaction with cybersecurity budgets.** Approximately 63 % of respondents from the energy and industrial sectors are satisfied with their cybersecurity budgets, with more than 60 % planning to increase their budget next year. In contrast, only 43 % of respondents in other sectors reported satisfaction with their cybersecurity budgets, with around half expecting a budget increase (Fig. 19).

Although phishing has long been the most prevalent attack method, a new trend observed was an increase in the sophistication of these attacks, similar to those seen in the financial sector. Respondents attributed the trustworthiness and sophistication of the phishing emails to the use of AI tools. However, less than half of the surveyed organisations in the energy and industry sectors conducted simulated phishing campaigns in 2023, with 35 % not testing resilience against cyber threats at all. This situation may be related to the respondents' perceptions of the severity of these attacks as minor. However, phishing is often the initial vector for cyberattacks.

**Satisfaction with the allocated cybersecurity budget, comparison of the energy and industry sectors vs. average (% of respondents)**

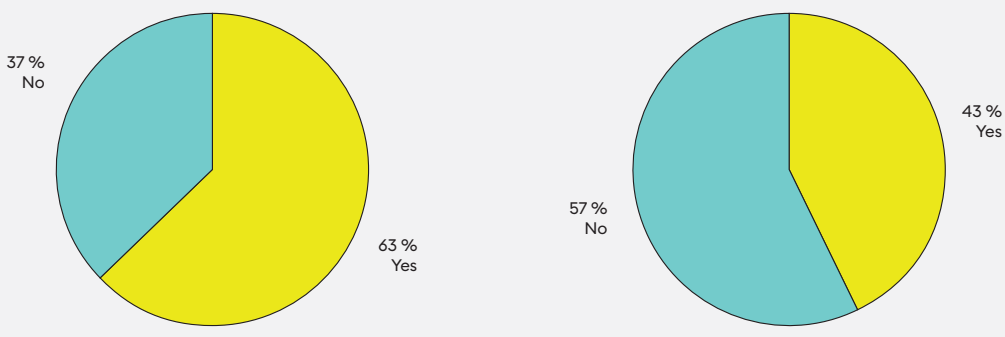
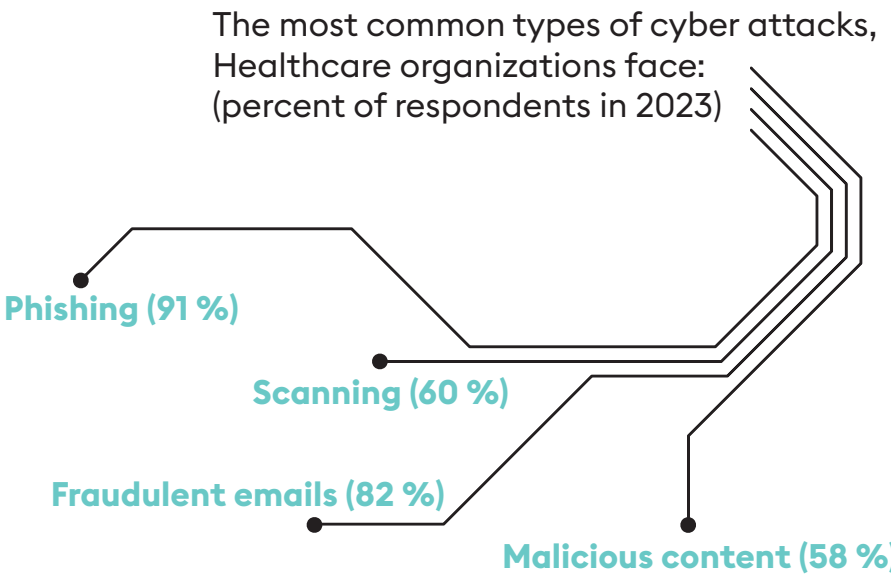



*Figure 19*

# Healthcare sector: Prevalent threats amid a decrease in ransomware attacks and insufficient resilience testing




**A decline in ransomware attacks in the healthcare sector was reported by 18 % of respondents, indicating a gradual long-term decrease.**

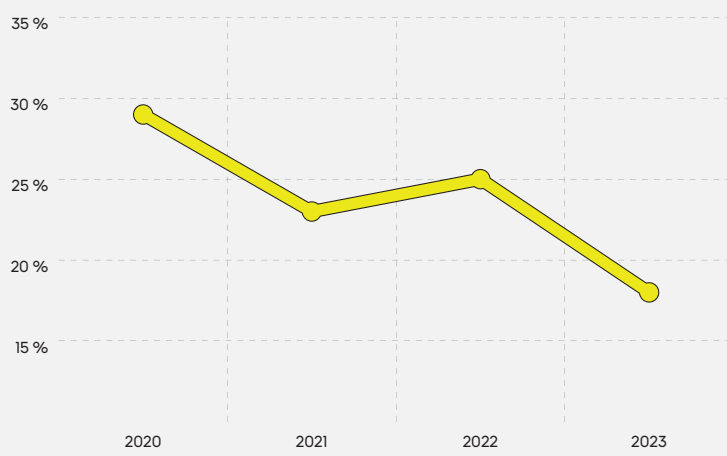
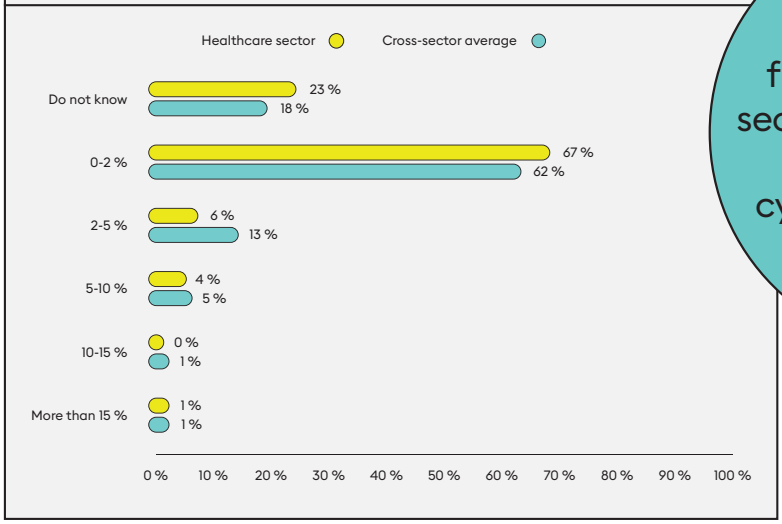



*Figure 20: Evolution of the number of healthcare sector respondents who reported ransomware attacks in a given year (regardless of the success of the attack) 2020–2023 (% of respondents)*

## Despite persistent threats, nearly half of healthcare organisations still do not test their staff's resilience to attacks.

In 2022, more than half (53 %) of the institutions surveyed did not perform any resilience testing. This number improved slightly in 2023, but 47 % of organisations still do not conduct any simulated phishing campaigns or penetration testing.

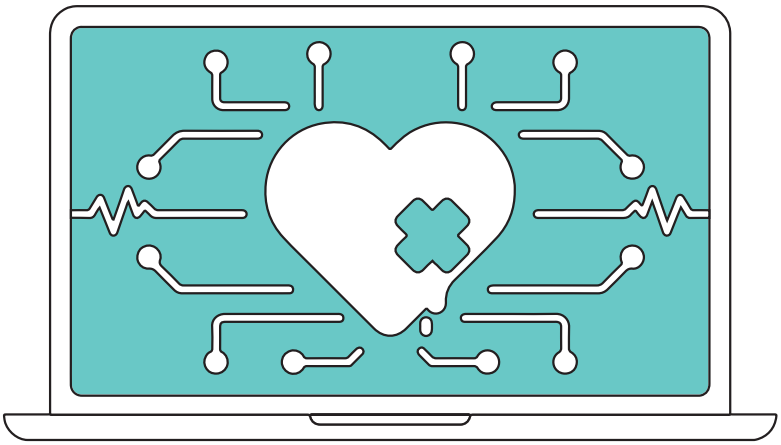
## Budget allocation for cybersecurity remains low, with 67 % of organisations spending 0–2 % of their budget in this critical area. This figure is notably worse than the cross-sector average.




61 % of respondents from the healthcare sector believe that their organisation's cybersecurity budget is insufficient.

*Figure 21: Proportion of total budget allocated to cybersecurity, comparison of organisation in the healthcare sector vs. average (% of respondents)*

In a more positive trend, 87 % of respondents reported an improvement in their organisation's level of cybersecurity compared to 2022 (definitely – 38 %, somewhat – 49 %), which may indicate a gradual sector-wide improvement in cybersecurity.



# Education:
# High exposure to cybercriminals and state-sponsored threats

State-sponsored groups frequently target academic research, with at least one Czech educational institution having reported and mitigated a malicious state-backed campaign in 2023.

**Comparison of the number of cyberattack attempts reported by respondents in the education sector (% of respondents)**

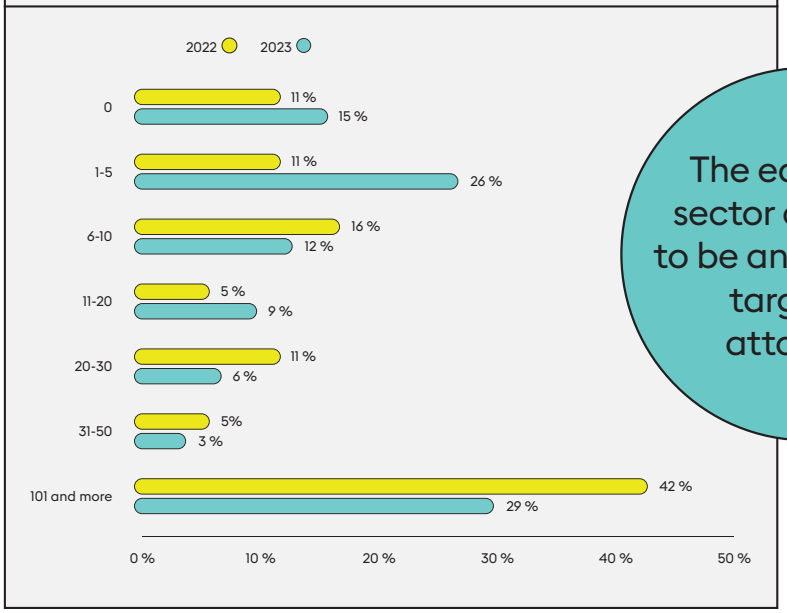



*Figure 22*

Despite an improvement over last year, this sector faces a larger volume of cyber incidents than any other (Fig. 22).

The education sector continues to be an attractive target for attackers.

This is most visible at both ends of the scale: the extreme category of over 101 incidents was 13 % higher than the average; instances of no attack at all were approximately 4 % below average (Fig. 23).

**A notable incident covered in the media involved the cybercriminal group Monti, which executed a ransomware attack on the Czech Republic's University of Defence (UNOB), detected on September 11.**

The attackers used double extortion, exfiltrating and encrypting the university's data and threatening to publish it if a ransom was not paid. **When the university refused, the group released documents containing the personal data of teaching staff, meeting minutes and study plans.** Information from such institutions can be valuable to malicious state actors. Although the university restored the encrypted data from backups, the theft of sensitive information constitutes a serious incident.

## Number of cyberattack attempts reported by respondents in the education sector vs. average (% of respondents)

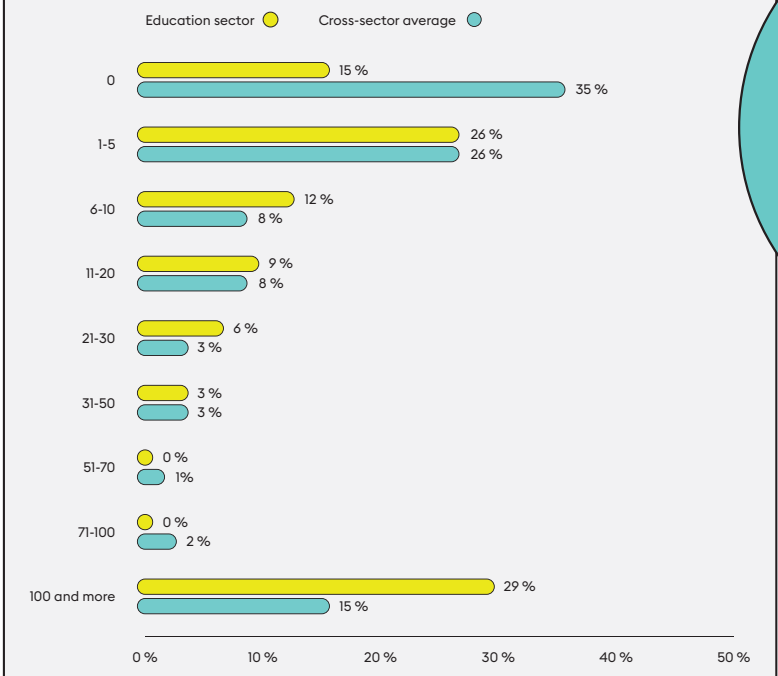



*Figure 23*

Phishing and fraudulent emails remain the most common vectors for attempted network intrusion and account for nearly two thirds of all reported attempts.

One method of reducing this risk is to test user resilience through simulated phishing campaigns. Compared to the previous year, more organisations in the sector are starting to conduct these types of campaign (Fig. 24). Surveyed respondents in the education sector reported that more than 67 % of all attack attempts did not trigger an incident. Despite this finding, the sector still trails the average and exhibits vulnerability.

## Comparison of education sector organisations' approach to testing employees against cyber threats compared to the cross-sector average (% of respondents)

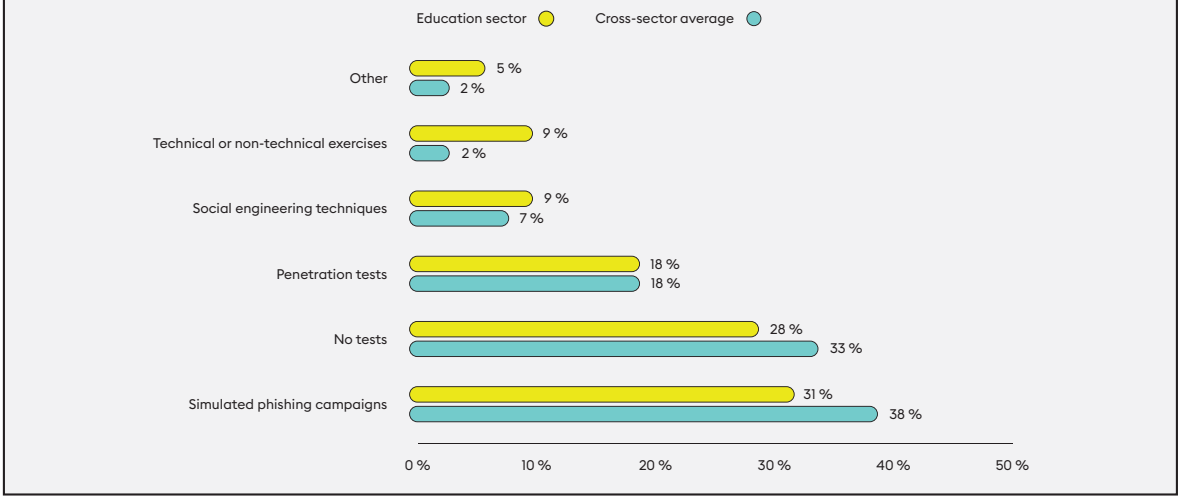



*Figure 24*

# Timeline of key warnings and alerts issued by NÚKIB in National cybersecurity level

## February

**Vulnerability in OneNote used to activate malware**

NÚKIB warns against an active phishing campaign that exploits a vulnerability in Microsoft OneNote, allowing a script to be executed when a file is opened. When activated, the script downloads malware to create a backdoor for an attacker to remotely access the user's system.

## March

**TikTok threat warning**

NÚKIB issues a warning concerning the threat of installing and using TikTok, citing its own analysis and findings and information from partners about possible security threats stemming from the app's user data collection and processing practices and function in the context of the legal and political environment of the People's Republic of China.

## June

**Heightened risk of ransomware attacks**

NÚKIB issues an alert highlighting increased cybercriminal activity involving ransomware. The alert includes details of vulnerabilities exploited by attackers and descriptions of the usual compromise vectors. NÚKIB also updates its document Ransomware: recommendations on mitigation, prevention and response, which provides comprehensive information and recommendations for this type of threat.

## July

**Vulnerability in MikroTik RouterOS**

A critical vulnerability (CVE-2023-30799) identified in MikroTik RouterOS routers allows attackers to potentially escalate privileges through a brute-force attack on login and password combinations. NÚKIB posts an alert and recommended mitigation measures for this threat.

## October

**Vulnerabilities in Cisco IOS XE**

Two critical vulnerabilities in the Cisco IOS XE operating system interface are discovered. The first (CVE-2023-20198) reaches the highest possible severity score of 10, the second (CVE-2023-20273) scores 7.2. NÚKIB issues alerts for each.

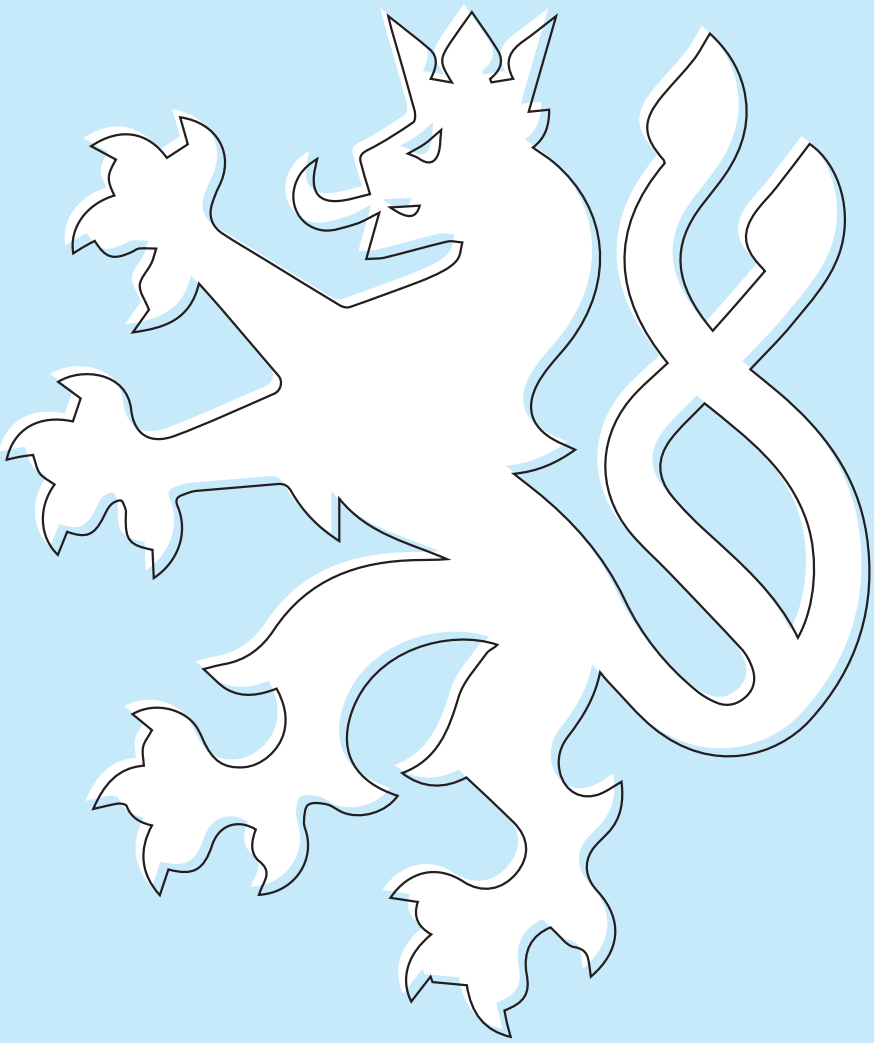
## November

**WeChat application threat**

NÚKIB issues an alert about the cybersecurity risks associated with using the WeChat mobile app and its Chinese version Weixin, offered by Tencent. Justified concerns point to a possible misuse of data collection practices, with the potential for accurately targeted cyberattacks, and the app's function in the context of the legal environment of China, similar to the concerns with TikTok.

# National cybersecurity level

4



# Project BIVOJ

In 2023, NÚKIB continued developing the project BIVOJ in cooperation with partners.

The project aims to establish a single, functional, secure shared platform providing security and communication services to public sector institutions, which would connect gradually to the system. Although the project is still in strategic development phase, some of its components are already being implemented.

**Under the coordination of the Deputy Prime Minister for Digitalisation and in close cooperation with NÚKIB, central government bodies are migrating to the uniform state domain gov.cz. This uniform domain will improve user-friendliness for citizens, provide legal certainty, and fortify resilience against DDoS attacks.**

# Supply chain security

The introduction of this mechanism should significantly reduce the impact of supply chain threats, such as supply disruptions caused by foreign states exerting their influence over suppliers, to key national ICT infrastructures.

**As mandated by the State Security Council in June 2022, NÚKIB is developing a supply chain security screening mechanism for state authorities to evaluate and mitigate risks associated with technology suppliers for strategically important infrastructure.**

The mechanism, under development as part of the new Act on Cybersecurity, includes mandates for NÚKIB and other relevant national authorities to screen suppliers and restrict the procurement of ICT supplies from suppliers deemed as high-risk.

The proposed process for the screening and mitigation of threats applies to critical security supplies only and includes provisions for infrastructure managers to comment on proposed supplier restrictions and exemptions for suppliers of non-substitutable technologies to avoid undesirable impacts.

The draft mechanism was finalised in 2023, and following inter-departmental consultation, merged with the Act on Cybersecurity to advance to the next legislative stages.

# Quantum threat mitigation

Quantum computer development is proceeding rapidly and sparking great interest among professionals and the public alike. **As the capabilities of quantum computers grow, they pose an increasing threat to current cryptographic standards.**

In response, NÚKIB has issued supporting documents (overview, minimum requirements for cryptographic algorithms, annex to the minimum requirements) explaining the nature of this threat and describing steps to mitigate the risks faced by cryptographic protection and cybersecurity in the coming years.

# Coordinated vulnerability disclosures

NÚKIB finalised its draft of the national coordinated vulnerability disclosure policy (CVD), including a detailed legal analysis of its relevant legal aspects. The NIS 2 Directive, which came into force at the end of 2022, introduced specific CVD obligations for EU member states.[6]

These were taken into account in NÚKIB's draft of the new Act on Cybersecurity, designating the Government CERT as the CVD coordinator, allowing any person to anonymously report vulnerabilities in ICT products.

[6] Directive (EU) 2022/2555 of the European Parliament and of the Council of December 14, 2022, on measures for a common high level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.

# Legislative anchoring:

# The new Act on Cybersecurity

**The NIS 2 Directive, published at the end of 2022**, expands the degree of harmonisation of cybersecurity regulation in the European Union, necessitating significant revisions to the Czech Republic's current statutory framework for cybersecurity.

**Due to the extensive changes introduced by NIS 2 that must be transposed into national law, a decision was made to draft a new Act rather than amend the existing one.** This new legislation, initiated by NÚKIB, integrates insights gained from the application of Act No. 181/2014 Coll. and feedback from entities governed by its provisions.

As in the previous year, the main themes in 2023 were negotiations and drafting of the new law, consultations with stakeholders (regulated entities and administrators of regulated sectors) and the public, and the launch of the formal legislative process. **NÚKIB also continued a comprehensive information campaign on the draft law through dedicated websites, lectures and responses to numerous enquiries.**

# European cybersecurity certification schemes

**The introduction of European cybersecurity certification schemes represents a step towards unifying and strengthening security standards in the European Union's digital space.**

Three certification schemes are being developed: EUCC (European Union Common Cybersecurity Certification Scheme on Common Criteria), EUCS (European Cybersecurity Cloud Certification Scheme) and EU5G (EU 5G Cybersecurity Certification Scheme).

Steady progress was made throughout 2023, culminating in the publication of the EUCC Implementation Act (IA EUCC) at the end of January 2024. Discussions regarding the draft candidate EUCS are ongoing at the ECCG (European Cybersecurity Certification Group) level, and the 5G candidate scheme is expected to be presented during 2024.

# NÚKIB supervisory activities in 2023

In 2023, NÚKIB's inspection and audit activities were influenced, as in 2022, by an escalating geopolitical situation, prompting a continued focus on examining the cybersecurity of key entities that support state functioning and provide essential services to citizens.

A total of twenty audits and inspections were carried out under the Act on Cybersecurity and its Implementing Decree No. 82/2018 Coll., on security measures, cybersecurity incidents, reactive measures, cybersecurity reporting requirements and data disposal (the Cybersecurity Decree), as amended.

**In addition to standard inspections, a comprehensive audit was also conducted. This audit exceeds the verification of organisational status through traditional surveys, interviews and device configuration checks and includes penetration testing, vulnerability scanning and tabletop exercises.**

Multiple NÚKIB departments, including the Audit Department, Government CERT, and the Exercise and Education Department, collaborate on these comprehensive audits, providing organisations with thorough feedback on their cybersecurity status and preparedness for potential incidents.

In cooperation with CZ.NIC, an audit of the gov.cz domain was also conducted in accordance with the Government of the Czech Republic's Resolution No. 23 of January 11, 2023. This resolution pertains to the intention to migrate to a uniform domain and the establishment of a uniform visual identity for central government bodies.

# Cybersecurity exercises:

**12**
**National Exercises**

**1645**
**Number of participants**

**3**
**International Exercises**

## TELCO23

In 2023, NÚKIB placed a significant focus on the telecommunications sector, organising October's TELCO23, a non-technical tabletop exercise for representatives of selected telecommunications service providers.

The aim was to verify the existence of security processes that minimise potential damage from cyberattacks and to establish proper communication protocols with the public, the media and within the organisation itself. This two-day exercise brought together government representatives and regulated entity representatives to discuss cybersecurity in the telecommunications sector and explore opportunities for cooperation.

## Comm Czech 2023

**In August, the Comm Czech 2023 communication exercise aimed to verify the reachability of designated contact persons within entities regulated under the Act on Cybersecurity.**

Up-to-date and readily accessible contact details are crucial during crisis situations, when timely and effective communication with regulated entities is critical to preventing the spread of damage.

## Locked Shields

Internationally, significant cybersecurity exercises were also held in 2023, including the well-established Locked Shields exercise in April, organised by the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia.

## Cyber Coalition

The Cyber Coalition exercise, a regular international cybersecurity event organized by NATO, was held in November.

# Cybersecurity prevention, awareness-raising and education in the Czech Republic

Cybersecurity prevention, awareness-raising and education remain crucial areas for boosting cybersecurity and societal resilience, in line with the objectives in the National Cybersecurity Strategy 2021–2025.

**It is imperative for Czech citizens across all social groups to be equipped to use digital technologies safely while navigating the online world.**

### Elementary schools

At the primary education level, the Revised Framework Programme (RVP) for primary education was deployed in 2023. Primary schools were required to begin teaching under the revised RVP, which includes new computer science curricula, at the latest by September 1, 2023.

### Universities

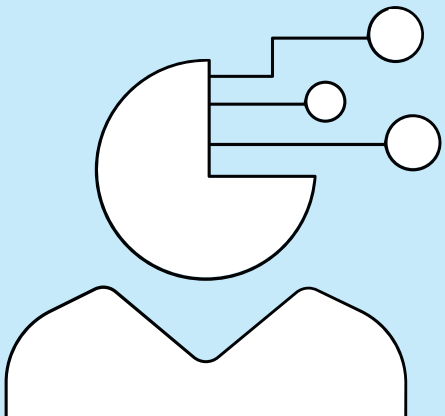
At the university level, a trend of moderate growth continues in the number of students enrolling in ICT programmes. However, slow growth in the number of cybersecurity-specific study programmes currently running or in preparation remains a concern.

### Vocational secondary schools

Similarly, the Framework Programmes for secondary vocational education were amended, effective from September 1, 2023, with a new computer science concept that includes a cybersecurity component.

### Retraining education

Improvements were made to the retraining education system. The Ministry of Labour and Social Affairs (MPSV) published a retraining database that consolidates available retraining courses, including those in cybersecurity courses, into a single, easily navigable location. This database improves access to necessary training for individuals interested in pursuing careers in cybersecurity.



### CyberCon 2023 Conference

In September 2023, NÚKIB held the ninth annual CyberCon conference at the Faculty of Social Sciences, Masaryk University, and the Faculty of Business and Economics, Mendel University.

The conference's main objective is to create a platform for connecting the public, academic and private sectors to discuss cybersecurity. During the three-day programme, approximately 350 participants attended lectures and discussions that covered technical, political and legal aspects of cybersecurity.

Based on the positive feedback from the previous year, an introductory workshop was included at the start of the conference. The second day concentrated on recent developments in regulation, including the new cybersecurity law, risk analysis in public procurement, and other relevant topics concerning the obligations of entities under NÚKIB. The third day was dedicated to public policies, featuring the introduction of new state institutions such as DIA and NCTEKK, and included discussions with political representatives on current cybersecurity issues.

# International cooperation:

## Following up on EU Czech Presidency successes

In 2023, NÚKIB built on the successes of the Czech Presidency of the Council of the EU (CZ PRES) by advancing the EU Council conclusions on ICT supply chain security, culminating in the creation of the ICT Supply Chain Toolbox. This toolbox is designed to include a set of general measures aimed at reducing critical risks to ICT supply chains.

At the EU Council, NÚKIB was involved in discussions for a proposed regulation, subsequently adopted at the end of 2023, aimed at establishing measures for a common high level of cybersecurity across EU institutions, bodies, offices and agencies.

The Council also adopted a general approach towards the draft Cyber Resilience Act and opened negotiations for the new Cyber Solidarity Act and an amendment to the Cybersecurity Act. By the end of 2023, the Council had adopted its mandate for further negotiations on the latter two.

## EU-CyCLONe

With the NIS 2 Directive coming into effect, in which NÚKIB has an active role, a network of liaison officers and relevant cyber crisis management offices (EU-CyCLONe) was established.

## ENISA Support Action

NÚKIB also acts as a contact point for the EU Cybersecurity Agency ENISA and facilitated the ENISA Support Action pilot project in 2023 to improve the cybersecurity of regulated entities in the Czech Republic.

## Counter Ransomware Initiative

NÚKIB participated in the Counter Ransomware Initiative, which adopted a joint statement in autumn 2023, endorsed by over 40 nations, including the Czech Republic, opposing ransomware payments. NÚKIB also played a significant role in preparing the national position on the application of public international law in cyberspace, a task led by the Ministry of Foreign Affairs, with ongoing cooperation to promote foreign policy in the EU and the UN.

## Prague Cyber Security Conference

Preparations for the 2024 Prague Cybersecurity Conference (PCSC) began in 2023, with the Prague Cybersecurity Meeting in June featuring international participation. Scheduled for the first quarter of 2024, the PCSC builds on previous editions and is expected to attract a broad global audience.

**Through its cyber-attachés, NÚKIB represents the Czech Republic's cybersecurity interests within the EU and the NATO Cyber Defence Committee. NÚKIB also contributes to the work of the NATO Cooperative Cyber Defence Centre of Excellence.**

As part of developing bilateral relations, NÚKIB took part in several high-level meetings, with foreign activities in the Indo-Pacific region now managed by a cyber-attaché based in Canberra, Australia. Bilateral relations with key partners in the EU, the US and Israel continued to develop. Cooperation with Ukraine also progressed significantly, with NÚKIB increasing its participation in development projects, such as CYBERVAC, organised by the Ministry of Foreign Affairs. Government CERT staff also visited Bosnia and Herzegovina to conduct several computer security training sessions.

# Government CERT activities:

## Development of the Threat Hunting Network

In 2023, NÚKIB advanced its projects designed to fortify the Czech Republic's cybersecurity and information security.

**A major new initiative was the launch of the Network Threat Hunting service, which provides contractual, pro-active detection of malicious activity and operational deficiencies within partners' infrastructure over a specified period.**

Once internal testing had concluded, a pilot probe was deployed within a regulated entity, and related processes were developed from the information obtained. Conceptual development of the Host Threat Hunting service also commenced in 2023, with plans for a pilot project launch next year.

## Development of forensic analyses

**NÚKIB also expanded its technical services with certification in early 2023 of the Analytical Information System for the forensic analysis of reported incidents involving classified information.**

This improvement augmented the capabilities of forensic analysis technicians, especially in the areas of mobile devices and cloud technologies.

## Capacity building in industrial and management systems

**In view of the conflicts in Ukraine and Israel, NÚKIB intensified its work on building long-term capacity, focusing on industrial control and management systems.**

In 2023, the primary focus was on audit and inspection activities within the gas industry and the telecommunications and energy sectors. NÚKIB also provided technical consultations to private entities likely to be identified as part of critical information infrastructure in the future. Specialists from NÚKIB consequently underwent internal training within those organisations and participated in the functional evaluation of internal security policies.

## Development and rebranding of the NÚKIB Portal

**In 2023, NÚKIB continued developing its non-public web platform, which was rebranded to "NÚKIB Portal".**

The platform disseminates non-public information to regulated entities and partners. This year, new public authorities and entities that manage critical information infrastructure or important information systems were enrolled on the platform.

These consisted mainly of entities from the transport sector, universities, regional authorities and official state bodies. In total, 71 organisations were enrolled, with plans to register additional entities ongoing.

## Strengthening penetration testing

**Last year, NÚKIB also reinforced its penetration testing activities. In addition to improving testing techniques, the Agency introduced a new physical penetration test service for evaluating the physical security, worker behaviour and building security at an organisation.**

The continuous vulnerability scanning service was also enhanced, enabling ongoing monitoring for known vulnerabilities through automated scanning tools.

# Outlook on cybersecurity trends in the Czech Republic for 2024 and 2025

## Cyberattacks through the supply chain

As predicted in the 2021 Report, cyberattacks targeting supply chains have increased, affecting the Czech Republic, **and are almost certain (90–100%) to remain a highly attractive vector for attackers.**[7]

Organisations heavily reliant on a single key supplier should be particularly vigilant.

**It is very likely (75–85%) that not only primary suppliers but also secondary and tertiary suppliers will be compromised more frequently than before.** Given the sophistication required, this vector is very likely (75–85%) to be used primarily by state actors.

## Geopolitically motivated cyberattacks

Cyberattacks against state institutions and critical infrastructure by state actors are almost always motivated by events in the physical world rather than mere financial gain or exploiting weak security.

Historically, NÚKIB has observed cyberattacks by state actors linked to the political stance of the Czech Republic or specific events (e.g., DDoS attacks by Russian-affiliated hacktivists).

**It is almost certain (90–100%) that this trend will persist, with attackers primarily seeking to gather information. It cannot be ruled out (25–50%) that some malicious actors will also attempt to infiltrate networks of major organisations and companies to exploit access for other destructive purposes in the event of conflict.**

## Generative artificial intelligence and large language models

**The year 2023 saw significant advancements in generative artificial intelligence (GenAI), particularly chatbots based on large language models (LLMs), such as the groundbreaking ChatGPT.**[8]

These AI chatbots and the products derived from them were rapidly adopted across many types of organisations. The methods to exploit them, such as generating phishing content or writing malicious code, emerged just as quickly. Despite efforts by service operators to limit the abilities of chatbots to produce malicious outputs, the potential to bypass these restrictions (known as jailbreaking) has consistently proved greater.

**In 2024, it is almost certain (90–100%) that the use and capabilities of AI services will expand.** New services will be introduced, and the functionalities of existing ones will continue to grow. The ability of operators to filter malicious queries is not expected to significantly improve in 2024, and therefore an increase in attackers' capabilities is anticipated. Specifically, a higher proportion of generative outputs beyond text, for example images, audio, video and deepfakes, is expected. **Chatbots are increasingly incorporating these capabilities, therefore an increase in audiovisual phishing forms, such as vishing, and other sophisticated phishing schemes combining various formats is expected.**

---

7 Worth mentioning are, for example, the compromise of authentication service provider Okta, software company JetBrains or Microsoft. In the latter two cases, state-sponsored actors were behind the malicious activities.

8 Although ChatGPT was launched in late November 2022, the massive surge in its popularity can only be dated back to early 2023.

# Annex 1:

# Evaluation of fulfilment of objectives specified by the 2023 National Research and Development Plan on Cybersecurity and Information Security

## Involvement in EU programmes and support for research projects

In 2023, support for priority research in cybersecurity and information security continued under the National Applied Research and Experimental Development Support Programmes. At the EU level, NÚKIB actively participated in developing the Digital Europe and Horizon Europe work programmes, which provide stable support for developing quantum technologies, artificial intelligence and other key research areas.

Acting as application guarantor, NÚKIB supported several research projects financed by public competition programmes of the Ministry of the Interior and the Technology Agency, the aim being to increase the practical applicability of research and development initiatives.

## Developing information facilities and connecting the cybersecurity research and development community

NÚKIB has also been instrumental in building information resources and fostering a research and development community. The agency's website features regularly updated cybersecurity research and development news and a recently created information page highlighting the activities and services of the National Coordination Centre for Research and Development in Cybersecurity.

Regular meetings of the Cybersecurity and Information Security Research and Development Centre further strengthened links between the academic, public and private sectors.

## International activities and cooperation - PROPED

Internationally, NÚKIB co-organised three research missions under the PROPED Economic Diplomacy Support Facility. The first mission in Germany focused on deepening cooperation between academia and the public sector in fibre network security. This was followed by a Czech-Bavarian networking seminar on cybersecurity in Regensburg, addressing the implementation of the EU NIS 2 Directive and challenges in the use of AI tools.

The third mission to Singapore was organized to exchange experience and establish contacts between Czech and Singaporean entities involved in cyber threat detection.

## Evolution of the National Coordination Centre

In accordance with Regulation 2021/887 of the European Parliament and of the Council, NÚKIB progressed towards establishing the National Coordination Centre. Two EU grants obtained by NÚKIB through the Digital Europe Programme will fund the improvement of information support services for providing advice and disseminating research and development results within the Czech Republic.

These projects will also facilitate financial support to entities active in cybersecurity through subsidies.

# Annex 2:

# Implementation of the Action Plan on the National Cybersecurity Strategy of the Czech Republic 2021–2025

The year 2023 marked the third year of evaluation for the Action Plan on the National Cybersecurity Strategy of Czech Republic 2021–2025 (the "Action Plan").

NÚKIB has a pivotal role in coordinating evaluation of the entire Action Plan and is responsible for or collaborates on 101 out of 105 tasks.

Several factors may negatively impact the implementation rate of the Action Plan. Under the Action Plan, some tasks are prioritised according to time and the capacity of the responsible authorities. Limited financial capacity or other internal organisational challenges within responsible authorities or collaborating entities may also affect the progress and completion of tasks.

**Eighty-five tasks were evaluated for 2023. Seventy-one tasks were either completed or continually fulfilled.**

**Fourteen tasks were only partially completed and will carry over to 2024. In 2022, nine tasks were partially completed, indicating a slight decrease in the task completion success rate for 2023.**

**No tasks were assessed as unfulfilled in 2023.**

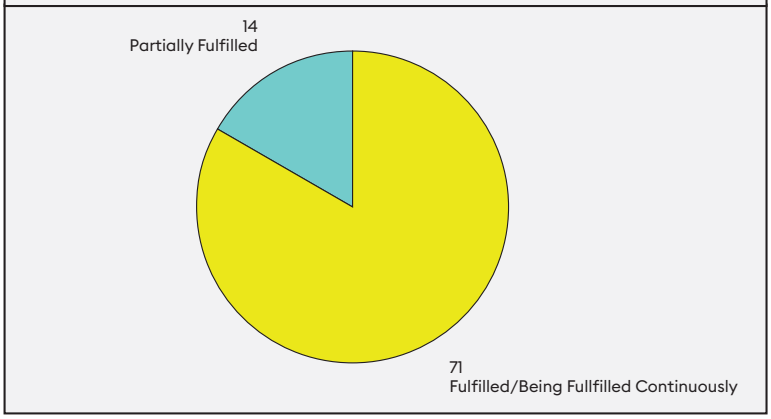


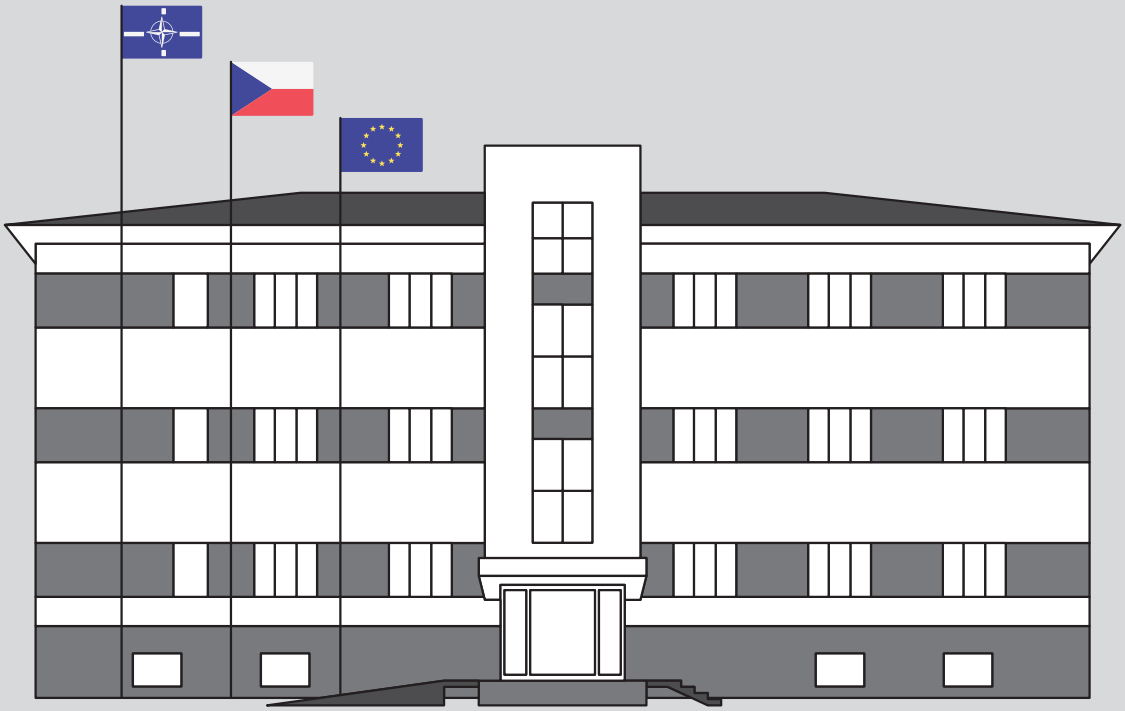

*Figure 25: Implementation of the Action Plan during 2023*

**An example of a task due and completed in 2023 is Task 40:**
*"Perform a legal review of the state of cyber hazards in the context of other crisis scenarios and prepare proposals for possible legislative changes."* The state of cyber hazards was revised under the proposal for a new CSA. This included a revision of crisis legislation in cooperation with the body responsible for crisis management, the Directorate General of the Fire Rescue Service of the Czech Republic. The legislation on cyber hazards was successfully reworded.

**An example of a task only partially completed is Task 83:**
*"Develop a concept for the protection of sensitive non-classified information."* NÚKIB conducted an analysis of the status quo and after discussion with internal and external partners, prepared an internal draft concept for the protection of non-classified information. However, the draft has not yet been approved. This task will be carried over to 2024 for further discussion with external bodies and submission to the security council.

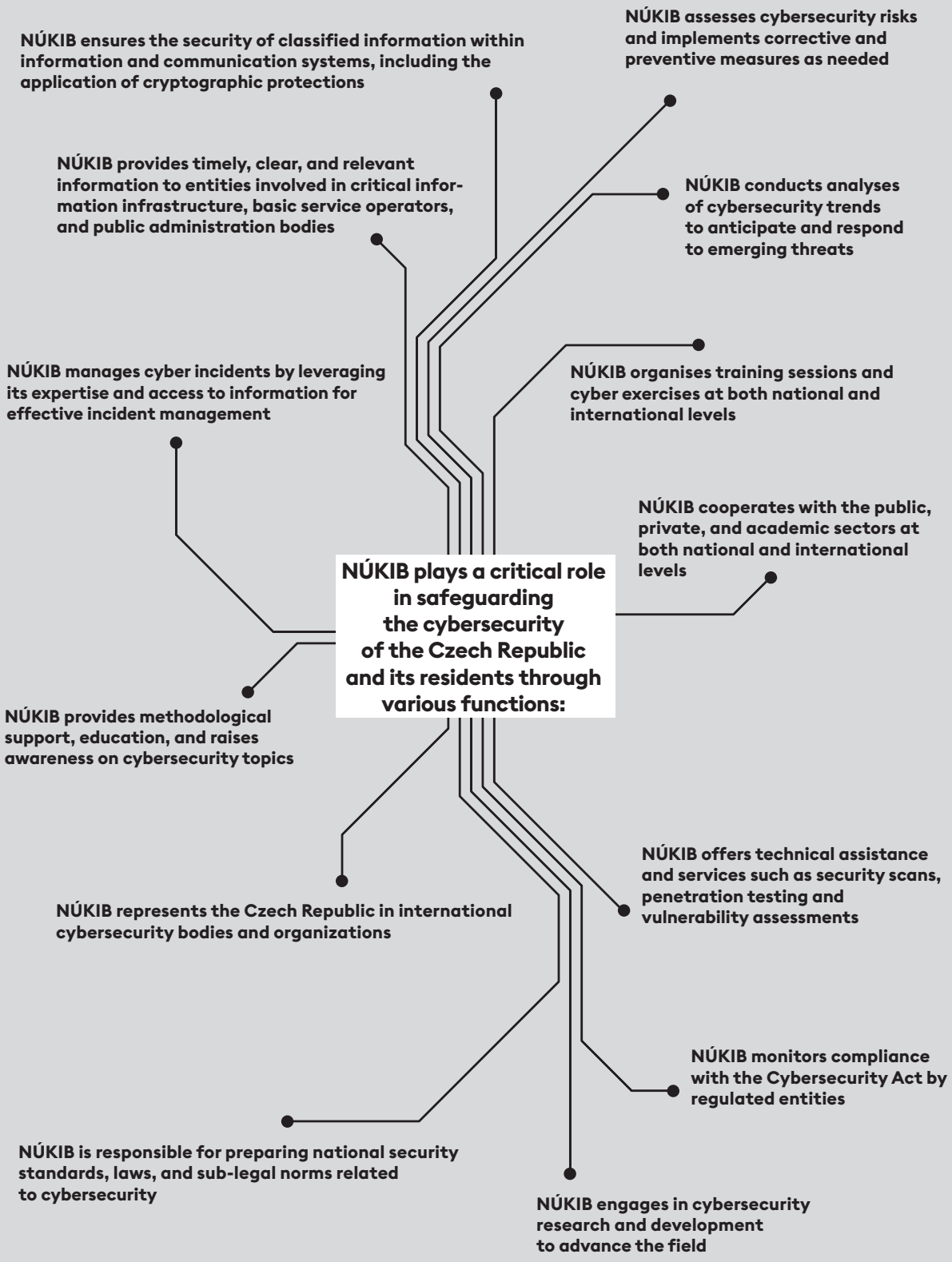
**The Action Plan also includes interim tasks that are evaluated annually.**
**For example, Task 67:**
*"Participate in and actively contribute to the organisation, preparation and conduct of international exercises and actively support the network of major cybersecurity partners through joint cyber exercises."* In 2023, the Czech Republic, through NÚKIB and other bodies, participated in organising and executing several international exercises (e.g., Cyber Coalition, NATO CMX 2023). Its participation in these activities is expected to continue.

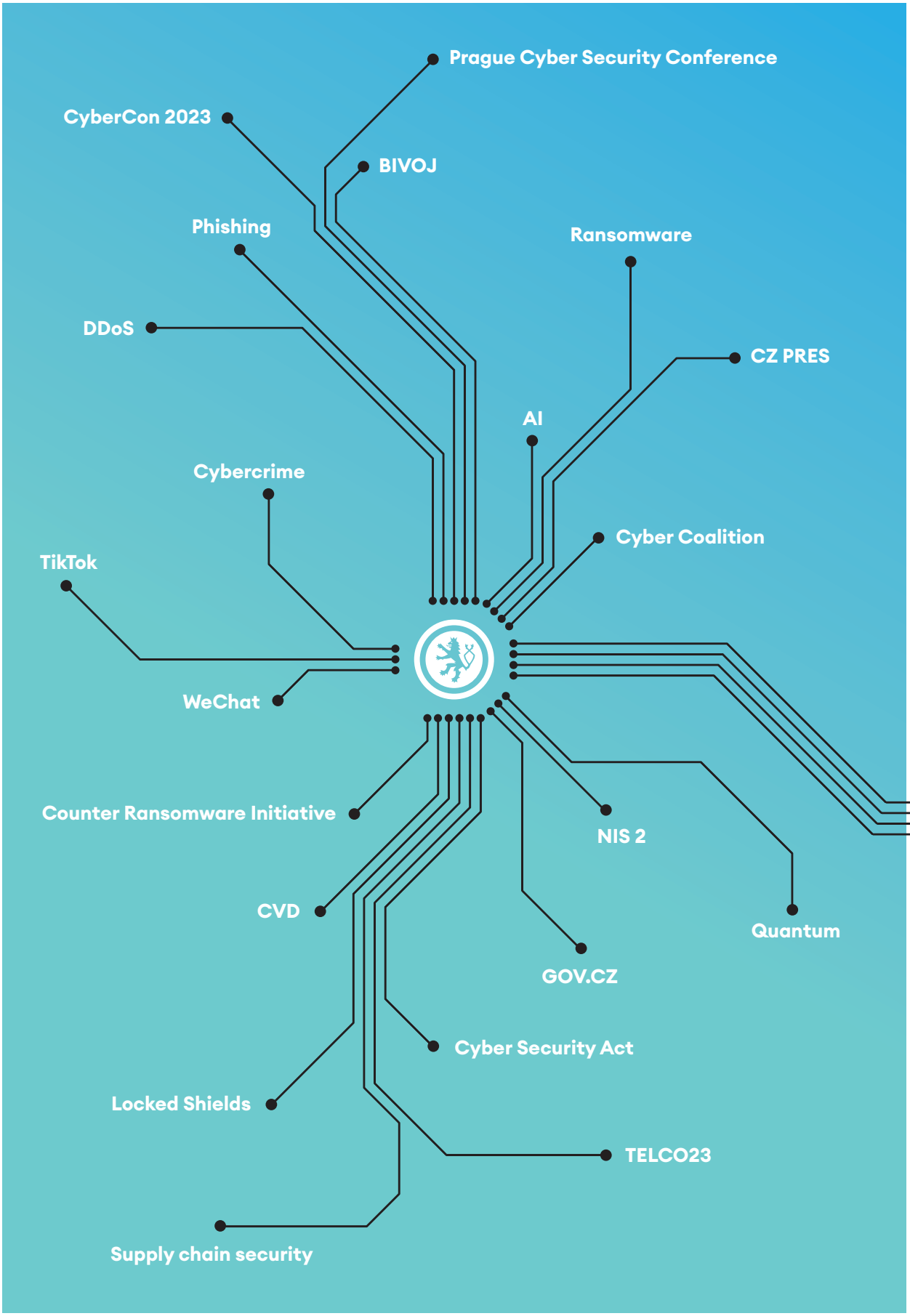
# About NÚKIB



**NÚKIB (National Cyber and Information Security Agency) is the central administrative body for cybersecurity in the Czech Republic. It is tasked with the protection of classified information contained in information and communication systems and ensuring cryptographic security. NÚKIB also oversees the Galileo global navigation satellite system, which is a public regulated service. Established on August 1, 2017, NÚKIB was created under Act No. 205/2017 Coll., amending Act No. 181/2014 Coll., on cybersecurity and on amendments to related acts (the Cybersecurity Act).**

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


NÚKIB ensures the security of classified information within information and communication systems, including the application of cryptographic protections
NÚKIB assesses cybersecurity risks and implements corrective and preventive measures as needed
NÚKIB provides timely, clear, and relevant information to entities involved in critical information infrastructure, basic service operators, and public administration bodies
NÚKIB conducts analyses of cybersecurity trends to anticipate and respond to emerging threats
NÚKIB manages cyber incidents by leveraging its expertise and access to information for effective incident management
NÚKIB organises training sessions and cyber exercises at both national and international levels
NÚKIB cooperates with the public, private, and academic sectors at both national and international levels
NÚKIB plays a critical role in safeguarding the cybersecurity of the Czech Republic and its residents through various functions:
NÚKIB provides methodological support, education, and raises awareness on cybersecurity topics
NÚKIB represents the Czech Republic in international cybersecurity bodies and organizations
NÚKIB offers technical assistance and services such as security scans, penetration testing and vulnerability assessments
NÚKIB monitors compliance with the Cybersecurity Act by regulated entities
NÚKIB is responsible for preparing national security standards, laws, and sub-legal norms related to cybersecurity
NÚKIB engages in cybersecurity research and development to advance the field


Prague Cyber Security Conference
CyberCon 2023
BIVOJ
Phishing
Ransomware
DDoS
CZ PRES
AI
Cybercrime
Cyber Coalition
TikTok
WeChat
Counter Ransomware Initiative
NIS 2
CVD
Quantum
GOV.CZ
Cyber Security Act
Locked Shields
TELCO23
Supply chain security