



Czech National
Cyber and Information
Security Agency

REPORT ON THE STATE
OF CYBERSECURITY
IN THE CZECH REPUBLIC

2025



DIRECTOR'S FOREWORD

Dear Readers,

From the perspective of cybersecurity and information security, 2025 was a year of significant shifts. Although there was a year-over-year decline in the total number of cyber incidents reported to NÚKIB after three years, it would be a mistake to interpret this trend as a weakening of threats in cyberspace. On the contrary, developments over the past year show that cyber threats are becoming increasingly sophisticated, more targeted, and, in many cases, more serious.

Ing. Lukáš Kintr

Director of the
Czech National
Cyber and Information
Security Agency



Despite a significant decline in DDoS attacks by hacktivist groups, availability attacks remain the most common type of incident recorded. Similarly, phishing continues to be the most widespread threat faced by the vast majority of us. These facts confirm that, in addition to technological, systemic, and legislative measures, the human factor, prevention, and systematic risk awareness campaigns are also of key importance.

The past year also brought a change in terms of the severity of reported incidents. The number of very important cyber incidents has increased, indicating that even amid an overall decline in incidents, the Czech Republic continues to face threats with potentially far-reaching consequences for the functioning of the state, its institutions, and the services they provide to our country's citizens.

The year 2025 was also of crucial importance in terms of the strategic and legislative anchoring of cybersecurity. For the first time, the government conducted a national attribution of a malicious cyber campaign—specifically, one carried out by a state-sponsored actor against the Ministry of Foreign Affairs. This step clearly demonstrates the state's readiness to respond openly to serious cyber threats. In this context, I would also like to mention two warnings issued by NÚKIB last year:

one regarding DeepSeek products, but more importantly, a broadly applicable warning about the threat posed by data transfers and remote administration originating from the People's Republic of China. Both warnings reflect the growing importance of strategic dependence on technology and the need to assess security not only from the perspective of individual products but also within a broader geopolitical context.

Another important milestone was the entry into force of the new Act on Cybersecurity and the launch of the NÚKIB Portal, which provides a unified tool for regulated entities to fulfill their legal obligations. Last September, the National Cyber Security Strategy was also approved, based on the principle of shared responsibility among the state, the public, private, and academic sectors, and individuals. It is precisely this ability to collaborate across society that will be one of the key prerequisites for the Czech Republic's resilience against cyber threats in the future.

I believe that, as it does every year, this report will provide a clear overview of the state of cybersecurity in the Czech Republic and that, as in previous years, it will help foster further interest in cybersecurity. I also believe that it will encourage further professional and public debate.

OBSAH

Director's Foreword	4
About the Report	8
List of Abbreviations	9
2025: Cybersecurity by the Numbers	10
Summary of the Report on the State of Cybersecurity in the Czech Republic in 2026	12
Cybersecurity in the Czech Republic in 2025 from the perspective of NÚKIB	13
Classification of cyber incidents reported to NÚKIB	15
Incidents from the perspective of the entities involved	18
Cybersecurity Spending: Less than half of the organizations considered their budget insufficient, but there were significant differences in the amount of funding they felt was needed	19
Experts and Users: There continued to be a shortage of qualified professionals in the labor market; users received regular training but were not tested sufficiently	20
Cyber threats and actors	23
State actors	24
Attribution and International Cooperation: Part of the response to the activities of Chinese and Russian Actors	24
Fraudulent schemes by actors linked to the Democratic People's Republic of Korea	25
Cybercrime	26
Targets of cyberattacks	27
Public sector: Consistently the main target of cyberattacks, with a significant increase in attacks carried out through service providers	28
Financial sector: A highly exposed sector that faces a large number of attacks but also has strong resilience and resources	29
Industry and energy: A sector seeing an increase in detected cyberattacks, but also a decline in their success rate	30
Healthcare: The number of attacks has declined, but the severity of potential consequences remains	31

Education sector: The decline in the number of detected cyberattacks in 2024 did not prove to be a trend	32
Timeline of selected alerts and warnings in 2025	34
National level of cybersecurity	35
The New National Cybersecurity Strategy and the development of an Action Plan to implement it for the period 2026–2030	36
National Legislative Framework	38
Act No. 264/2025, on Cybersecurity	38
EU Legislative Framework	40
Supervisory Activities	42
Cybersecurity exercises	43
International cooperation	44
NATO cooperation	44
New strategic relationships	44
Development cooperation and cyber capacity building	45
EU cooperation	45
Conferences	45
Government CERT activities	46
Outlook: Cybersecurity trends in the Czech Republic for 2026 and 2027	47
Annex 1: Evaluation of the fulfilment of the objectives of the National Research and Development Plan on Cybersecurity and Information Security 2025	50
Annex 2: Implementation of the Action Plan for the National Cybersecurity Strategy of the Czech Republic for 2021–2025	51
Annex 3: Implementing Regulations for the New Act on Cybersecurity	52
About NÚKIB	53

ABOUT THE REPORT

At the beginning of 2026, NÚKIB sent a questionnaire consisting of 63 questions to entities regulated under Act No. 181/2014, on Cybersecurity and on amendments to related laws, as amended, as well as to a number of other key institutions and organizations that were not regulated by the Act on Cybersecurity at the time the 2025 Report on the State of Cybersecurity in the Czech Republic (hereinafter the “Report”) was being prepared or that are still not regulated (Act No. 264/2025, on Cybersecurity, entered into force in November 2025, and the deadline for regulated entities to self-identify expired on December 31, 2025). The questions covered a wide range of topics, such as cyberattacks, cybersecurity costs, cybersecurity staffing, users, technologies, and established processes. A total of 425 entities completed the questionnaire, of which 338 were regulated and 87 were unregulated (pursuant to Act No. 181/2014). NÚKIB drew on the data obtained to compile the Report. All data from the questionnaires have been anonymized.

Evaluation process

The assessment of the state of cybersecurity in the Czech Republic is based on an analytical process that includes both the quantitative and qualitative evaluation of data from completed questionnaires, NÚKIB’s findings, information provided by partners, and other available open-source information. NÚKIB was unable to verify the data provided by respondents or to conduct a more in-depth verification of the statements made. The analytical conclusions contained in the Report are based on the premise that the responses in the questionnaires are not biased. We use probabilistic terms to express our analytical assessment (see below).

This report does not provide a complete list of all cybersecurity activities. The purpose of this document is to describe and assess the threats in cyberspace that the Czech Republic faced in 2025, as well as the activities that help mitigate them.

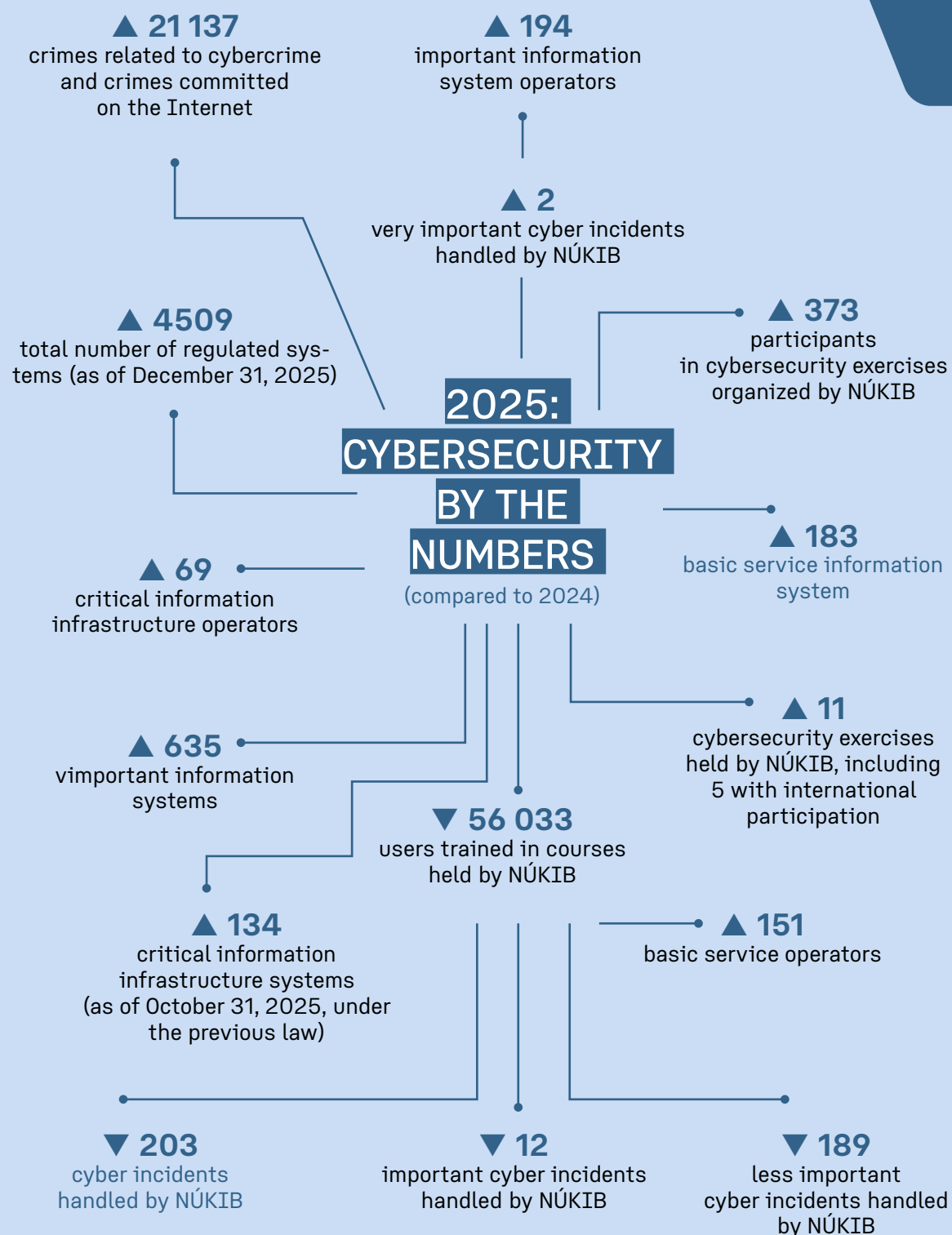
Probabilistic expressions used in the 2025 Report on the State of Cybersecurity in the Czech Republic

Probability expressions and their corresponding values as percentages:

Expression	Probability
Almost certainly	90–100%
Highly likely	75–85%
Likely	55–70%
Cannot be ruled out/Realistic possi-	40–50%
Unlikely	20–35%
Highly unlikely	0–15%

LIST OF ABBREVIATIONS

Action Plan	Action Plan for the National Cybersecurity Strategy for 2021–2025
AI	Artificial Intelligence
BIS	Security Information Service
CRA	Cyber Resilience Act
CSA	Cybersecurity Act
CVD	Coordinated Vulnerability Disclosure
DDoS	Distributed Denial of Service
DORA	Digital Operational Resilience Act
DPRK	Democratic People’s Republic of Korea
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUCC	EU Cybersecurity Certification Scheme on Common Criteria
GRU	Main Directorate of the General Staff of the Armed Forces of the Russian Federation, (Главное управление Генерального штаба Вооружённых Сил России)
ICT	Information and Communication Technologies
PAIS	Public administration information systems
IT	Information Technologies
JCSA	Joint Cyber Security Advisory
LLM	Large Language Model
NATO	North Atlantic Treaty Organization
NP CPCI	National Policy on Cryptographic Protection of Classified Information
NCSS	The National Cyber Security Strategy
NÚKIB	National Cyber and Information Security Agency
p.p.	Percentage point
PCSC	Prague Cyber Security Conference 2025
PRC	People’s Republic of China
Report	Report on the State of Cybersecurity in the Czech Republic
MI	Military Intelligence



Internal, external, and Wi-Fi tests identified 227 vulnerabilities, of which 18 were critical, 60 were high, 94 were medium, and 55 were low.

Over the past year, 36 penetration tests were conducted, including 8 internal tests, 11 external tests, 4 Wi-Fi tests, 6 physical tests, 6 phishing campaigns, and 1 load test.

Over 800 comments on the new cybersecurity law were submitted and addressed.

In 2025, we recorded more than 252,000 visits to the NÚKIB Portal.

In 2025, the Czech Republic ranked first among more than 140 countries in the National Cyber Security Index, published by the Estonian foundation e-Governance Academy.

We answered approximately 1,278 questions regarding the NIS2 Directive and other matters related to regulation and cybersecurity.

In 2025, two warnings were issued; no reactive or protective measures were taken.

SUMMARY OF THE REPORT ON THE STATE OF CYBERSECURITY IN THE CZECH REPUBLIC IN 2026

.....

In 2025, after three years, the number of cyber incidents fell from 268 to 203. This is largely due to a decrease in the number of incidents involving DDoS attacks by hacktivist groups. Compared to 2024, this type of attack fell to less than half of its 2024 level.

.....

According to the NÚKIB incident classification, attacks targeting availability, which include DDoS attacks, remained the most common type of incident (46%) in 2025. From the perspective of the survey respondents, the most common type of attack was phishing (50%), which was reported by 90% of respondents. Last year, the number of very important incidents increased by one, bringing the total to two.

From a cybersecurity perspective, 2025 was a landmark year for NÚKIB, particularly in terms of legislative anchoring, and for the Czech Republic in terms of national attribution.

In May of last year, the government conducted a national attribution of a malicious cyber campaign targeting the Ministry of Foreign Affairs, which was carried out by the Chinese state-sponsored actor APT31. NÚKIB participated in the investigation of the attack alongside domestic partners from the security community.

On November 1, 2025, Act No. 264/2025, on Cybersecurity (hereinafter the “Act on Cybersecurity”), came into effect, marking the completion of the drafting process for this key piece of legislation, which lasted three years, eight months, and nine days.

In this context, the new NÚKIB Portal was also launched, serving as a single point of contact for regulated entities to fulfill their legal obligations toward NÚKIB.

Two warnings were issued during the year, specifically regarding certain DeepSeek products and, in particular, the threat posed by data transfers and remote administration from the People’s Republic of China (hereinafter the “PRC”). Based on this warning, entities regulated under the Act on Cybersecurity must take this threat into account in their risk analyses and respond to the identified risks by adopting appropriate security measures.

The warning was largely groundbreaking, as it does not focus on a single technology but highlights a complex problem and is applicable to all industries, services, and devices.

In September, the government approved the National Cyber Security Strategy, which is based on the “whole-of-society” principle, aimed at bringing together all relevant stakeholders and creating a resilient environment capable of responding to large-scale crises, dynamic threats, and technological changes.



CYBERSECURITY
IN THE CZECH
REPUBLIC IN 2025
FROM THE
PERSPECTIVE
OF NÚKIB

CYBERSECURITY IN THE CZECH REPUBLIC IN 2025 FROM THE PERSPECTIVE OF NÚKIB

In 2025, NÚKIB recorded a total of 203 cybersecurity incidents, the lowest figure in the last three years. This decline was largely due to a significantly lower number of incidents related to DDoS attacks by hackers. Compared to 2024, this type of attack fell by less than half (from 167 in 2024 to 94 in 2025).

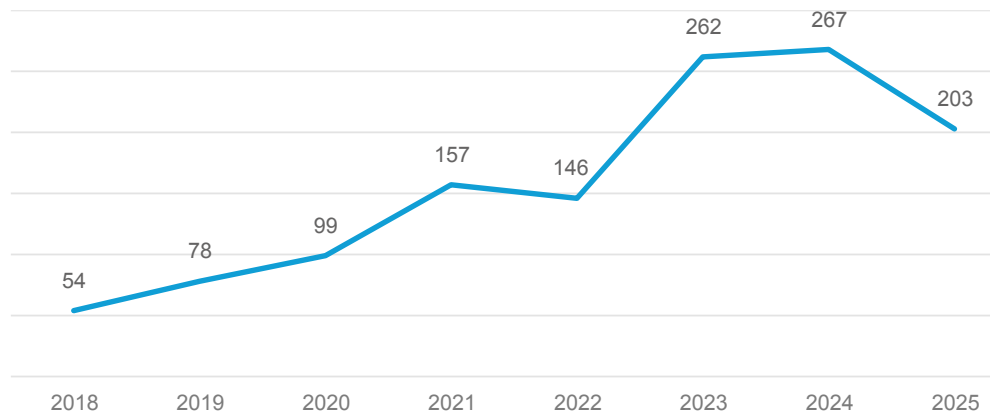
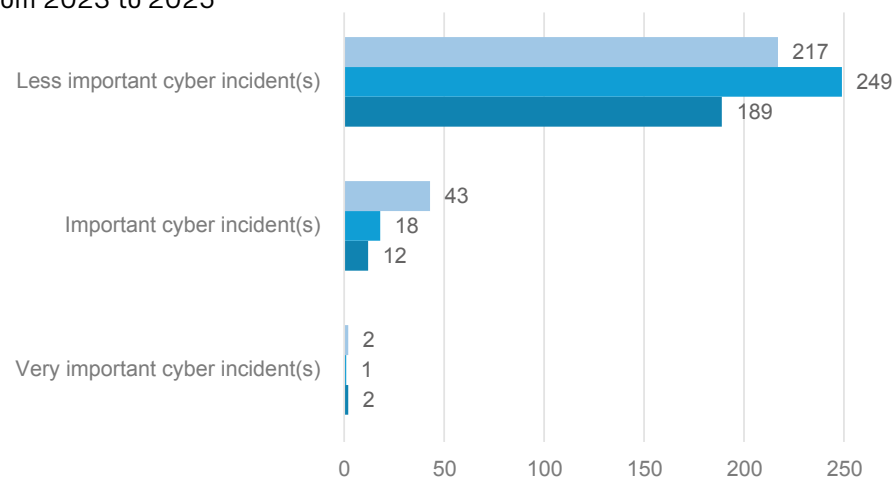


Figure 1: Trends in the number of incidents recorded by NÚKIB, 2018-2025

As for the severity of incidents, the number of very important incidents increased by one last year, bringing the total to two. NÚKIB recorded a total of 12 important incidents. The remaining incidents (189) fell into the category of less important incidents.

Figure 2: Year-over-year comparison of the severity of incidents recorded by NÚKIB from 2023 to 2025

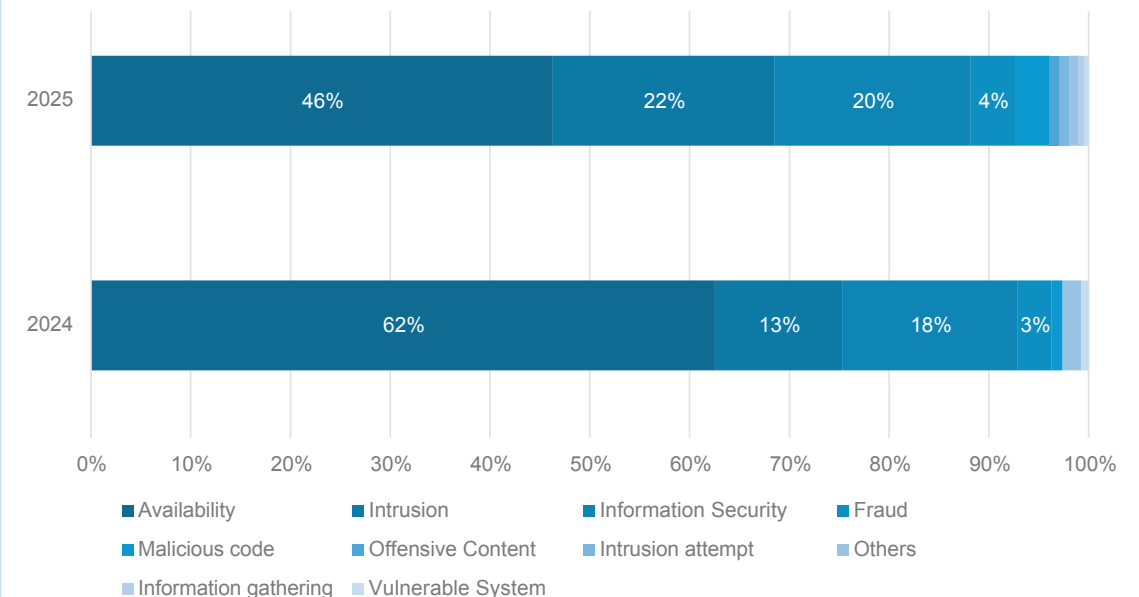


CLASSIFICATION OF CYBER INCIDENTS REPORTED TO NÚKIB

In terms of incident classification, incidents targeting availability have predominated for several years in a row, although their share has decreased significantly compared to the previous year.

Conversely, the number of breaches has increased, making them the second most common category. NÚKIB does not attribute the rise in breaches to any specific large-scale campaign; rather, it attributes it to a combination of circumstances. The next most common category was Information security, which primarily included ransomware attacks.

Figure 3: Percentage breakdown of categories within the incident classification system for 2024-2025



Availability – e.g., disruption of availability caused by a DoS/DDoS attack or sabotage

Intrusion – e.g., compromise of an application or user account

Information security – e.g., unauthorized data access, unauthorized information modification

Malicious code – e.g., a virus, worm, Trojan horse, dialer, or spyware

Fraud – e.g., phishing, identity theft, or unauthorized use of ICT

Intrusion attempt – e.g., an attempt to exploit a vulnerability, a login attempt, etc.

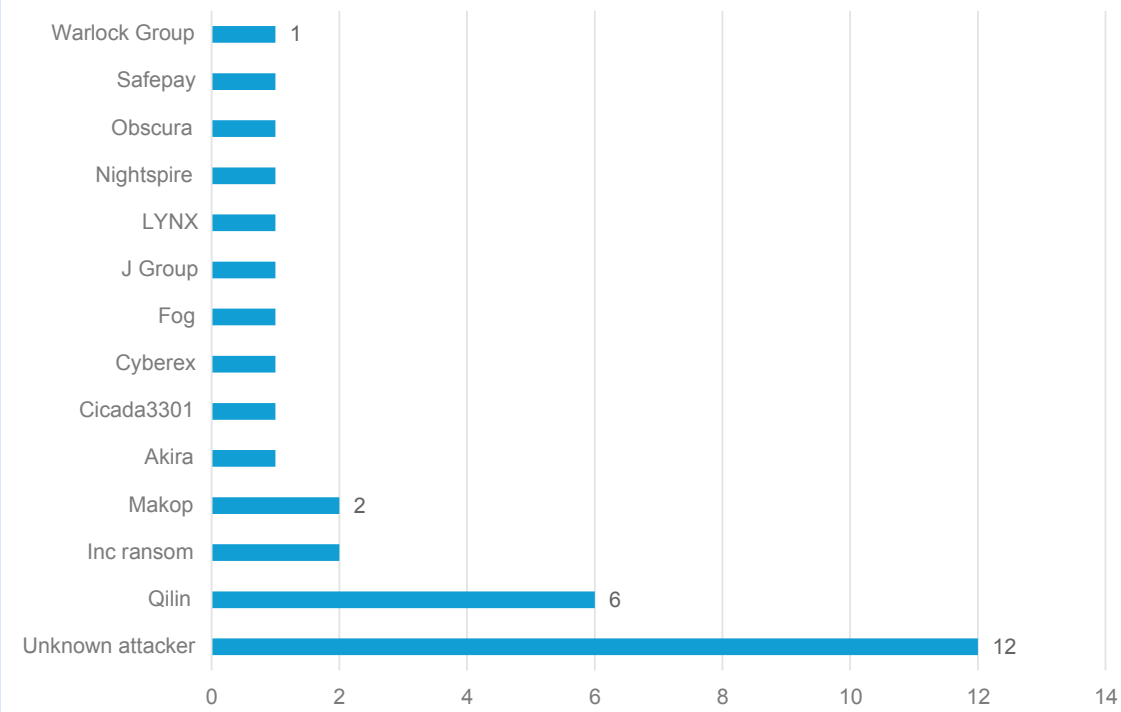
Information gathering – e.g., scanning, sniffing, or social engineering

RANSOMWARE ATTACKS

Ransomware attacks have long been among the most serious cyber threats. Ransomware gangs are primarily motivated by financial gain, which explains why they are not selective and target companies and organizations of all sizes across various sectors. During 2025, NÚKIB recorded ransomware-related incidents in sectors such as the public, education, healthcare, security, industrial, and technology sectors. The composition of the actors behind these attacks was equally diverse. **With the exception of the Qilin gang, which ranks among the most active ransomware actors globally, the other groups were responsible for only one or two attacks.**

In addition to the above, NÚKIB observed a trend of gradual change across the entire ransomware ecosystem. **As elsewhere in the world, a larger number of smaller ransomware groups were active in Czech cyberspace.** Furthermore, the entire issue was highly dynamic throughout 2025. Actors emerged, rebranded, merged, and so on at a rapid pace. As a result, it has become much more difficult to keep track of the modus operandi of each group.

Graf 4: Perpetrators behind ransomware attacks recorded by NÚKIB in 2025



Although DDoS attacks generally do not have as severe consequences as those of ransomware, they have long been the most common type of attack recorded by NÚKIB. This remained true in 2025, even though their number declined significantly during this period. There were significant developments in the field of hacktivism during the year. One of the key events was a joint international operation called Operation Eastwood, coordinated by Europol and Eurojust, which targeted the pro-Russian hacktivist group NoName057(16). The Czech Republic was among the countries that participated in the operation, which aimed to disrupt the group's infrastructure and activities. In July 2025, the operation resulted in the disruption of the group's key infrastructure and the issuance of several arrest warrants for individuals allegedly responsible for the group's activities.

However, NÚKIB had already observed a gradual decline in the activities of pro-Russian hacktivists prior to Operation Eastwood. For comparison, in the first half of 2025, NÚKIB recorded just under twenty incidents related to DDoS attacks, whereas in the second half of 2024, that number was nearly four times higher. **Although there was a slight increase in attacks in the third quarter, partly due to retaliatory attacks by hacktivists in response to Operation Eastwood, the total number of incidents related to DDoS attacks decreased by more than half year-over-year.**

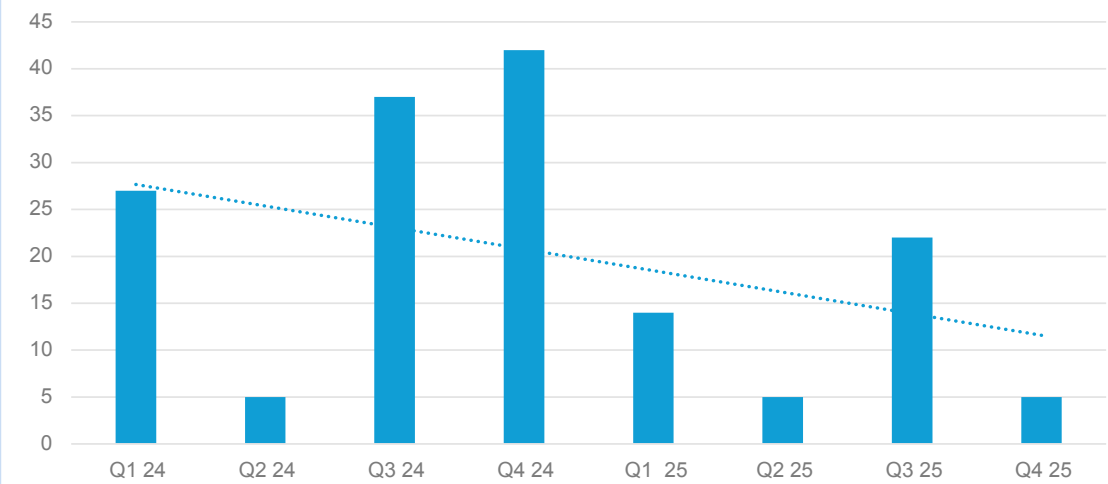


Figure 5: Quarterly trends in DDoS attacks, 2024-2025

Conversely, the trend of hacktivists targeting operational technology systems, which NÚKIB had already mentioned in its previous Report on the State of Cybersecurity, increased slightly. These attacks differ from DDoS attacks in that they do not aim merely to cause temporary unavailability, but instead generally seek to manipulate the targeted systems. Despite the slight increase, however, the number of cases remained low, consisting primarily of attacks against inadequately secured systems with devices exposed to the internet. None of the attacks resulted in significant damage, so overall this remains a minor trend.

INCIDENTS FROM THE PERSPECTIVE OF THE ENTITIES INVOLVED

In 2025, as in previous years, the most common types of attacks were phishing, fraudulent emails, and scanning, with respondents rating their severity as minor to marginal. Overall, the most serious types of attacks were malicious content, availability attacks (e.g., DDoS), and ransomware.

Respondents most frequently pointed out the increased sophistication of phishing attacks and their variants, including the possible use of artificial intelligence (hereinafter “AI”) tools to create them. At the same time, however, more than a quarter of the organizations surveyed did not test their employees at all (e.g., using fake phishing emails). Yet regular testing and awareness training are among the most effective tools for strengthening employees’ resilience against cyber threats.

Phishing, fraudulent emails a scanning remain the most common types of attacks

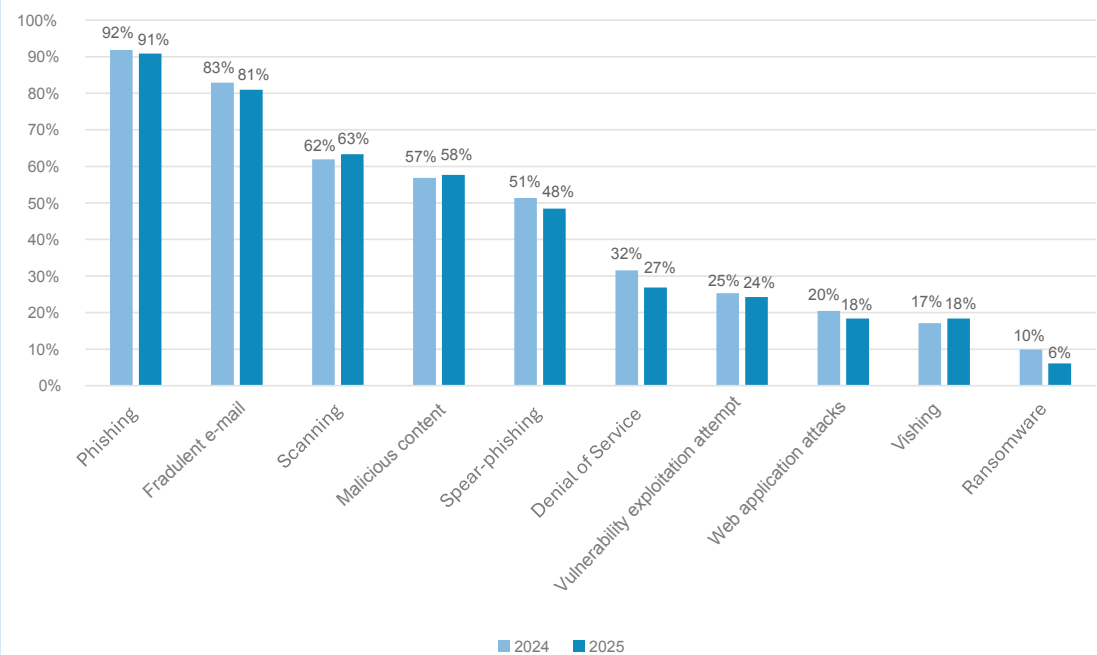


Figure 6: What types of attacks or attempted attacks did you record last year?

In terms of funding allocated to cybersecurity, 2025 marked a period of continued, mildly positive trends without any significant declines. Although approximately half of the surveyed entities (51%) still reported an increase in their cybersecurity budgets, stagnation was evident compared to previous years, as the proportion of these entities did not increase further. For the second year in a row, however, there was a growing number of institutions that considered their cybersecurity budgets to be sufficient (see Figure 7). Although this figure rose again in 2025, it unfortunately represents an increase of only one percentage point (hereinafter “p.p.”) and does not replicate the significant growth seen between 2023 and 2024. It therefore appears that this was not the beginning of a trend toward satisfactorily meeting the needs of the IT departments of the surveyed organizations, but merely a partial improvement.

Cybersecurity Spending: Less than half of the organizations considered their budget insufficient, but there were significant differences in the amount of funding they felt was needed

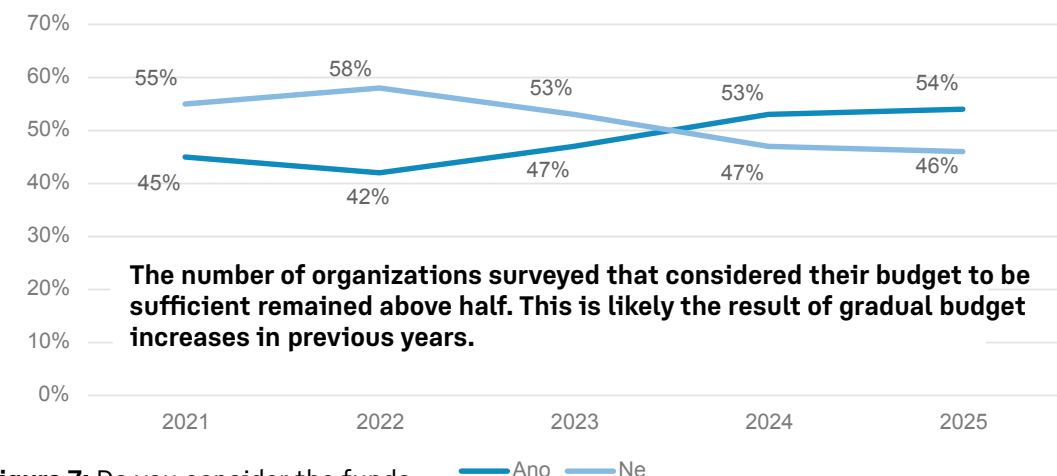


Figure 7: Do you consider the funds allocated to ensure your organization’s cybersecurity to be sufficient?

The second significant aspect was determining the necessary budget increase in cases where the current amount was insufficient. Over the long term, the majority of respondents have been unable to estimate by how much their budgets should be increased (see Figure 8). The difference between this group and the second most common response (0–10%) was 39 p.p. Difficulty in determining their actual needs and communicating them within the organization may also have played a role in the slow increase in budgets.

Regardless of their views about the ideal budget size, however, organizations with insufficient budgets agreed on specific priorities. The greatest investments were needed for new technological solutions and infrastructure security.

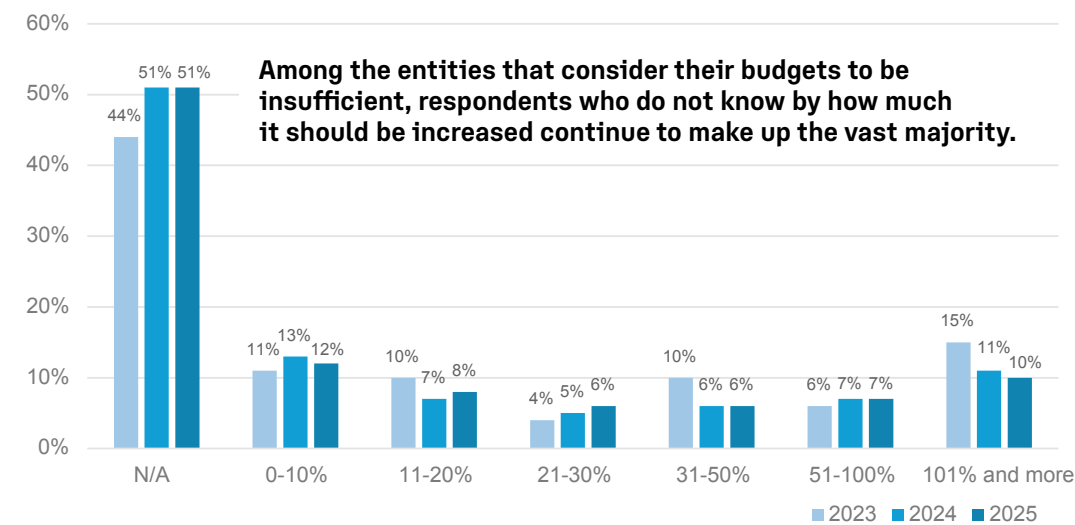


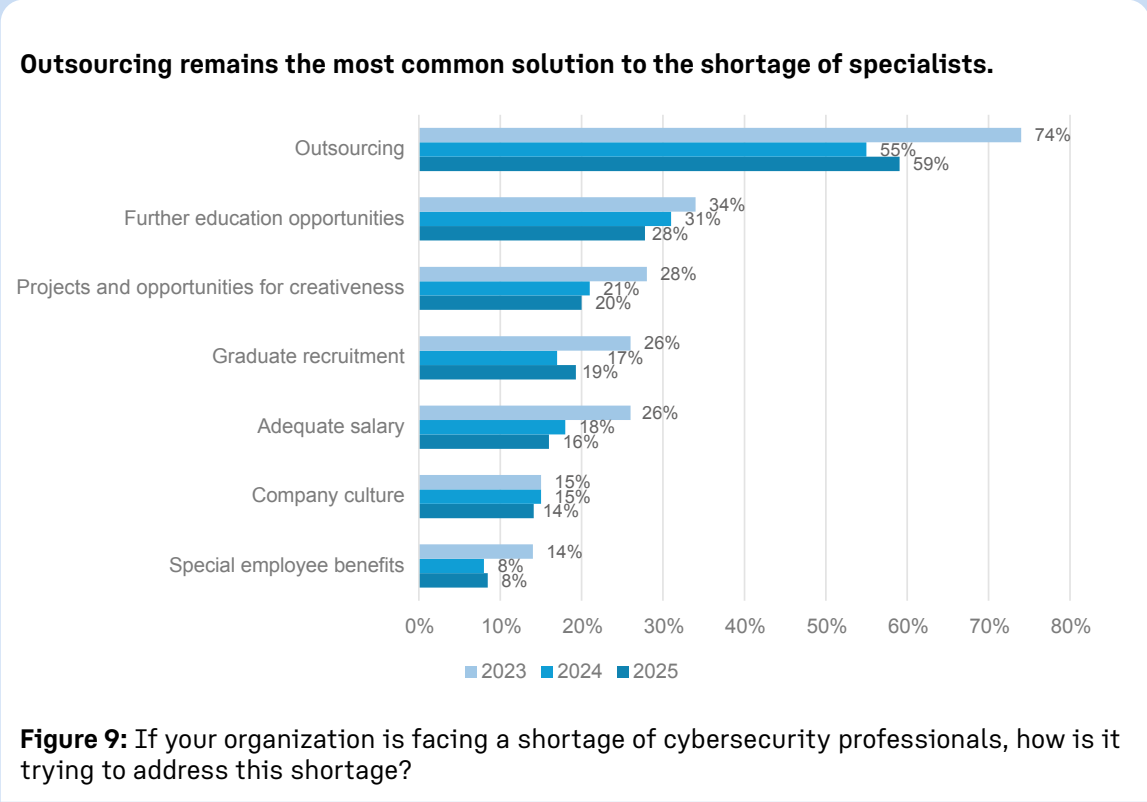
Figure 8: If you consider the cybersecurity budget to be insufficient, by what percentage do you think it should be increased?

EXPERTS AND USERS: THERE CONTINUED TO BE A SHORTAGE OF QUALIFIED PROFESSIONALS IN THE LABOR MARKET; USERS RECEIVED REGULAR TRAINING BUT WERE NOT TESTED SUFFICIENTLY

In 2025, the organizations surveyed continued to face difficulties in finding qualified cybersecurity professionals. According to the organizations surveyed, the overwhelmingly dominant factor deterring candidates was insufficient compensation (75%). The situation was worst in the public sector and in education, where 92% and 84% of organizations, respectively, cited compensation as the main obstacle.

Other factors included a lack of opportunities for personal or professional development (21%) and inadequate employee benefits (19%). Respondents also noted that the insufficient number of job seekers in the labor market represented a significant obstacle.

Organizations continued to address the shortage of qualified cybersecurity personnel primarily through outsourcing. They also sought to attract new experts by offering opportunities for continuing education and project involvement, although to a lesser extent than in previous years (see Figure 9).



Respondents ranked cybersecurity architects, SIEM security monitoring roles, network infrastructure administrators, server infrastructure administrators, and cybersecurity auditors among the five most difficult positions to fill.

One positive trend was the steadily increasing proportion of organizations that considered the funds allocated to training their specialists to be sufficient (70%). However, the proportion of organizations that allocate funds specifically for user training did not continue to rise. As a result, as many as 50% of organizations had to provide employee training without additional resources (see Figure 10).

Funds are allocated to training experts. In half of the cases, user training must be carried out without funding.

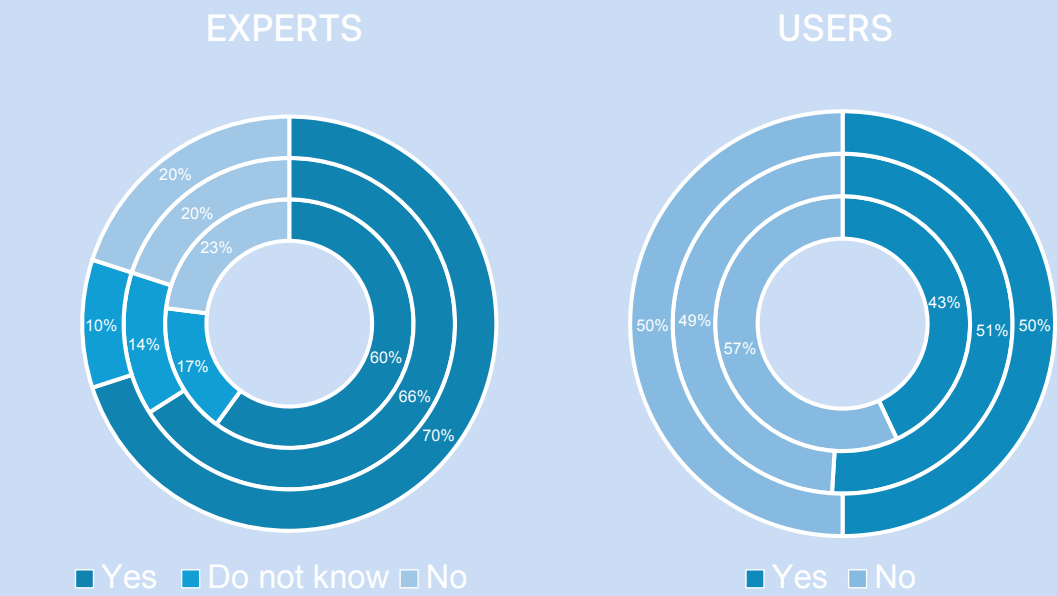


Figure 10: **Experts:** In your opinion, does your organization have sufficient financial resources to provide regular cybersecurity training for experts?
Users: Does your organization allocate funds each year specifically for cybersecurity training for all users?

Of the organizations that provide cybersecurity training to their employees, the proportion rose to 96%; training sessions are most often held once a year (56%) and 27% of organizations train their employees more frequently, while 17% do so less frequently.

The most common method of training continued to be providing employees with information, for example, via email or internal portals. Testing employees' cyber resilience most often took the form of simulated phishing campaigns, penetration testing, technical or non-technical exercises, or specific social engineering techniques (e.g., randomly placed USB drives). However, as many as 38% of organizations did not test their employees at all in 2025, and this percentage has not decreased significantly over the long term (see Figure 11).

Simulated phishing campaigns are the most common method of testing employees, but a significant number of organizations do not test their employees at all.

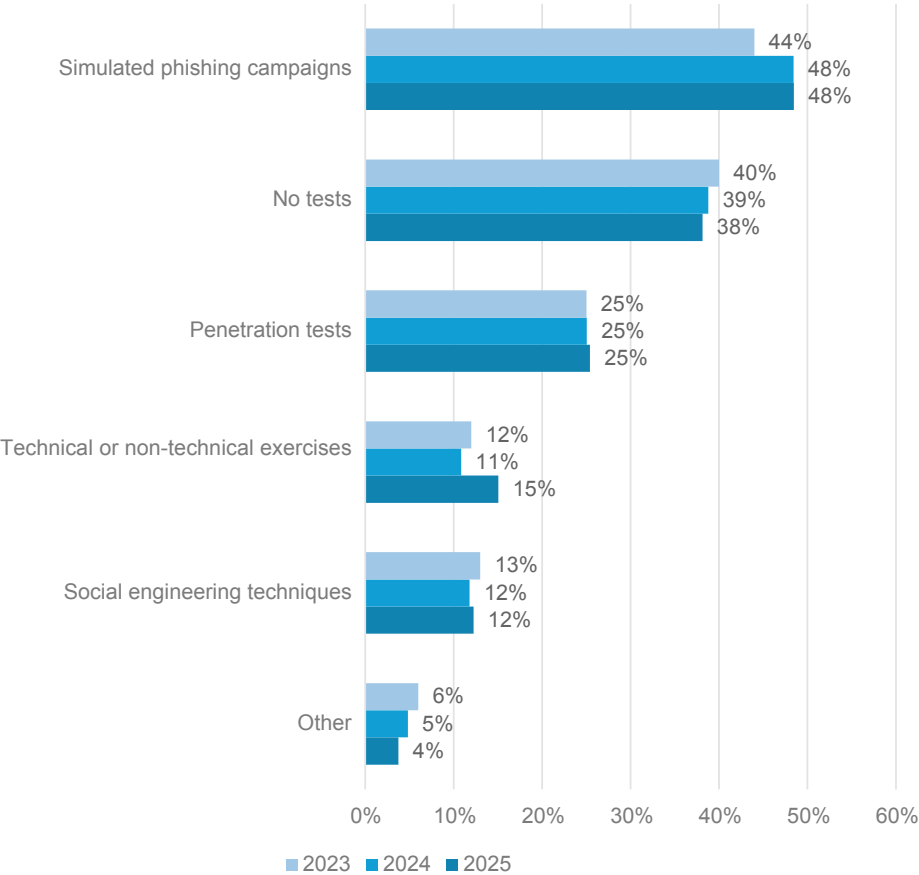


Figure 11: Do you test your employees' resilience against cyber threats?



CYBER THREATS AND ACTORS

CYBER THREATS AND ACTORS

STATE ACTORS

Attribution and International Cooperation: Part of the response to the activities of Chinese and Russian Actors

Chinese and Russian state-sponsored actors have long posed the most significant threat to Czech cyberspace, and their activities targeting Czech entities continued unabated in 2025. The Czech Republic continuously monitors, analyzes, and actively responds to these threats, including by officially identifying the perpetrators of attacks and condemning them. International cooperation and information sharing have also played a significant role in these efforts, serving as a crucial element in ensuring cybersecurity and responding to serious threats in cyberspace.

People's Republic of China

A major event in 2025 was the attribution of a cyberattack on the Ministry of Foreign Affairs to the APT31 group, which is linked to the Chinese intelligence service. The findings of an analysis conducted by NÚKIB, Military Intelligence (hereinafter “MI”), the Security Information Service (hereinafter “BIS”), and the Office for Foreign Relations and Information clearly indicate that the PRC is behind this long-term malicious campaign, which has been ongoing since 2022, and that it is highly likely (75–85%) that the campaign was conducted by the APT31 group (also known as Zirconium or Judgment Panda). APT31 has been linked to a wide range of attacks against political and other targets, including targets in the European Union (hereinafter the “EU”) and the North Atlantic Treaty Organization (hereinafter “NATO”). **The Czech government has unequivocally condemned this malicious cyber campaign against its critical infrastructure and called on the PRC to adhere to the principles of responsible state behavior in cyberspace, which have been endorsed by all member states of the United Nations.** In connection with the cyberattack against the Czech Republic, the EU and its member states, as well as all NATO allies, expressed their solidarity and support.

However, the cyberattack mentioned above was by no means the only activity by the Chinese state to which the Czech Republic responded during the past year. **NÚKIB, together with U.S. government security agencies and other international partners, joined a joint analysis (the Joint Cybersecurity Advisory, hereinafter “JCSA”) highlighting activities that partially overlap with those of an actor most commonly referred to as Salt Typhoon.** These activities included intrusions into networks around the world with the aim of gaining long-term access to them and using that access for espionage. The attackers targeted backbone routers of major telecommunications service providers as well as routers at the network edge of both the provider (provider edge) and the customer (customer edge). They then used compromised devices or trusted connections to further penetrate those networks.

Russian Federation

Among the threat actors linked to Russia, the most prominent was the long-running campaign by the Russian actor APT28, which operates under Russia’s military intelligence agency, the GRU. The response to this campaign was a joint JCSA, in which Czech security institutions, including NÚKIB, BIS, and MI, participated alongside partners from the United States, the United Kingdom, Germany, Poland, Australia, Canada, Denmark, Estonia, France, and the Netherlands. **The APT28 actor’s campaign targeted primarily logistics and technology companies involved in foreign aid to Ukraine, but it also affected government institutions in various countries, as well as IP cameras at border crossings and railway hubs in Ukraine and neighboring countries.**

At the end of 2025, NÚKIB, together with other national partners, joined the U.S. Federal Bureau of Investigation’s JCSA in response to cyberattacks by pro-Russian hacktivist groups targeting critical infrastructure. **Unlike advanced state-sponsored actors, these groups use less sophisticated methods with a lower impact, which can nonetheless result in damage to the compromised systems.** At the same time, these groups often do not understand the processes they are attempting to disrupt, which can lead to unintended consequences, including physical damage to systems.

Fraudulent schemes by actors linked to the Democratic People's Republic of Korea

A fraudulent scheme in which citizens of the Democratic People's Republic of Korea (hereinafter “DPRK”) pose as legitimate information technology professionals from other countries and secure remote positions is an innovative strategy that North Korean actors have successfully used to raise funds for the regime. At the same time, this scheme can also lead to data theft and subsequent extortion, or to cyber espionage. The entire scheme is carefully designed to avoid arousing the suspicions of potential employers during the hiring process. **This threat spread to Europe last year, where it was detected in Germany, Poland, and Hungary, among other countries.** The Czech Republic does not appear on the list of countries targeted by this campaign; however, the DPRK’s interest in domestic companies cannot be ruled out in the future (40–50%).

CYBERCRIME

In 2025, there was a 14% year-over-year increase in the number of cybercrimes compared to 2024. Specifically, there were 2,642 incidents.

Compared to the 2023–2024 period, when the number of recorded offenses fell by nearly 6% year-over-year, there was a renewed increase, which—apart from minor fluctuations—has been evident over the long term throughout the entire monitoring period.

In 2025, there was another increase in the number of cybercrimes; this is the highest number since this type of crime was first recorded.

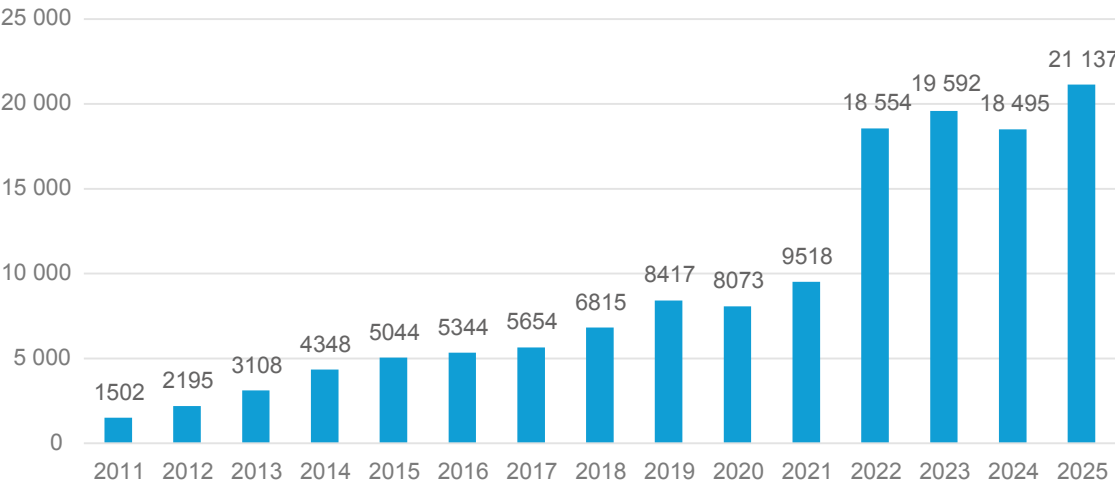
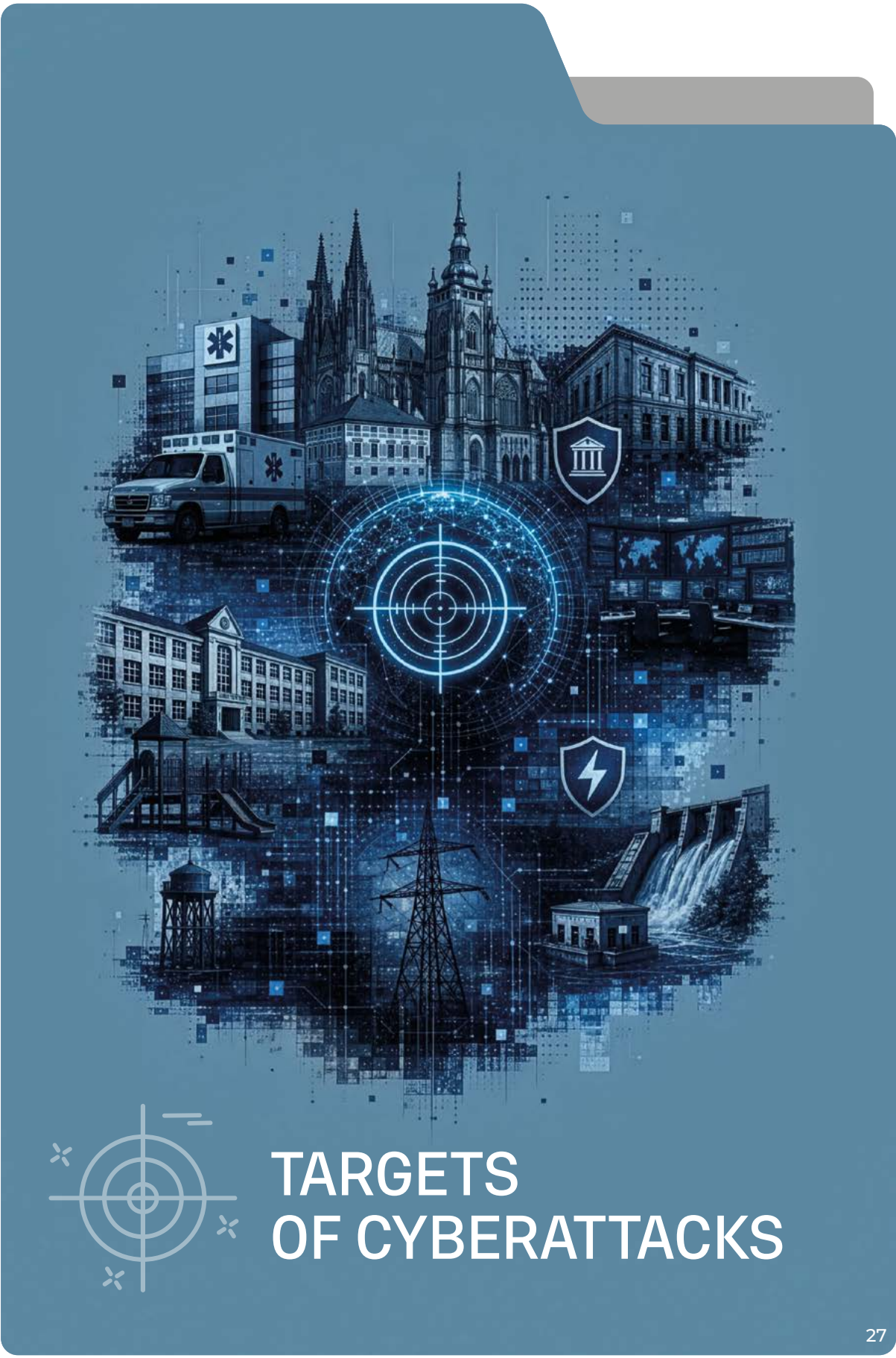


Figure 12: Recorded cybercrimes in the Czech Republic for the period 2011-2025

According to the classification of individual types of cybercrimes, fraudulent activity accounted for the highest proportion—for the umpteenth consecutive period. This is likely due to the use of increasingly sophisticated techniques, with the victims of fraud including not only individuals but also institutions, such as, among others, the case of the charity organization Tady a ted', which was defrauded in 2025.

The number of cybercrimes is thus on the rise, despite the resources allocated to awareness and education campaigns. In general, this increase is linked to the shift of criminal activity to cyberspace, a trend that can be observed worldwide.



TARGETS OF CYBERATTACKS

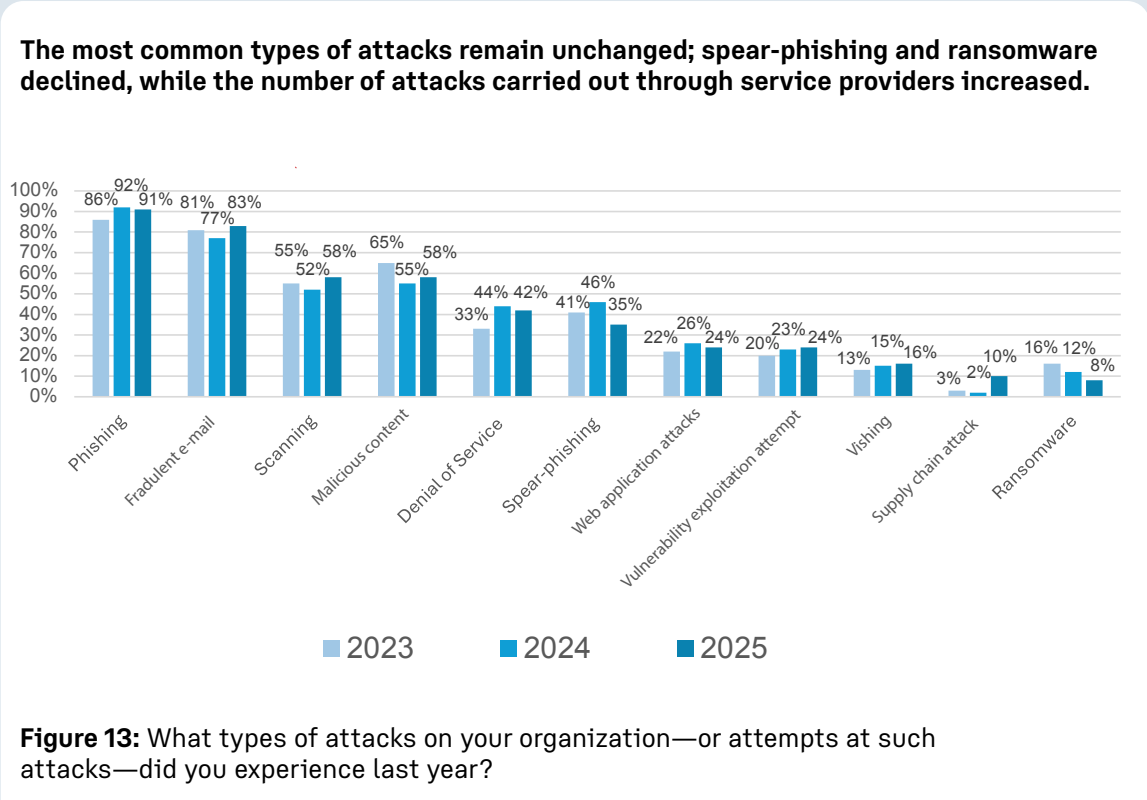
TARGETS OF CYBERATTACKS

PUBLIC SECTOR: CONSISTENTLY THE MAIN TARGET OF CYBERATTACKS, WITH A SIGNIFICANT INCREASE IN ATTACKS CARRIED OUT THROUGH SERVICE PROVIDERS

The survey shows that the public sector remained the most common target of cyberattacks in 2025 as well; however, the number of attacks remained similar to the number reported in 2024. **Once again, the most frequently reported types of attacks included phishing, fraudulent emails, malicious content, and scanning.** This situation may reflect the fact that, despite stated expectations, more than half of the respondents in the public sector did not see an increase in their cybersecurity budgets in 2025. In most cases, the budgets remained the same; however, contrary to expectations, the number of organizations that saw a decrease in their cybersecurity budgets actually increased.

Compared to previous years, there was a decline in the number of detected spear-phishing attacks and ransomware incidents; however, there was a notable increase in the number of attacks carried out through service providers. This finding is consistent with a broader global trend. **The increase in the number of cases reported by respondents may also be due to the success of cyberattacks against the software services of these service providers, or against the confidentiality of the data stored by these providers, which may include large multinational companies.** Whether this represents an anomaly or a new trend in the Czech context will only become clear in the future.

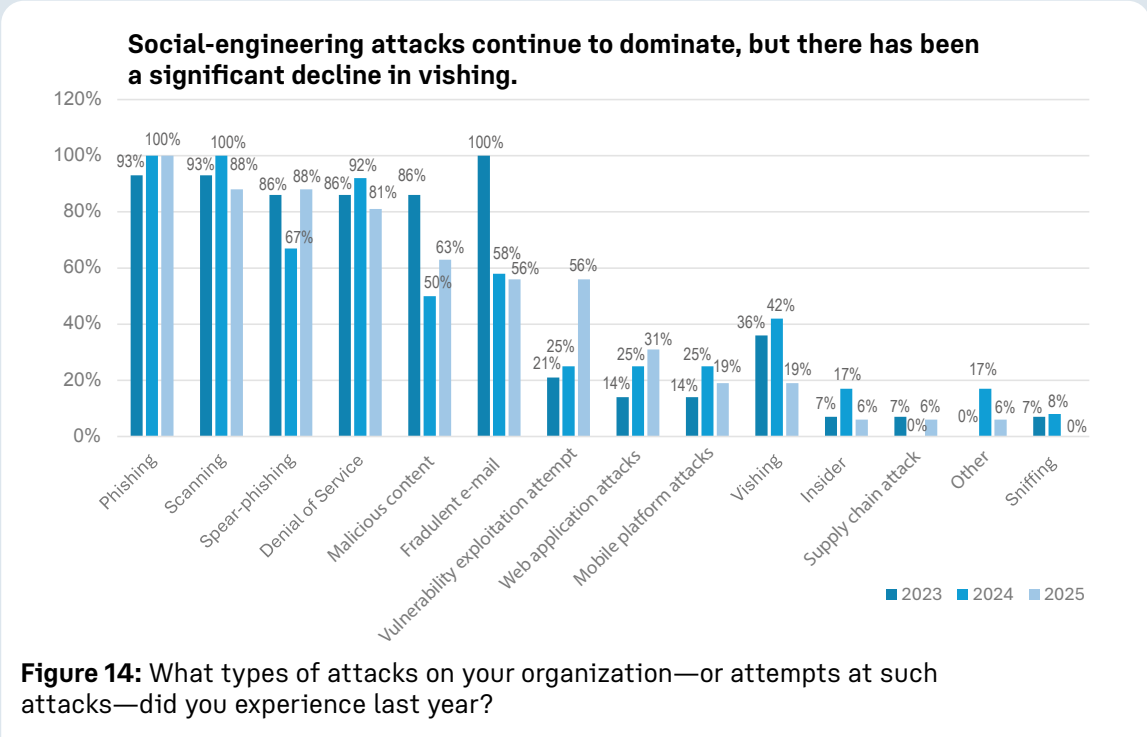
Just as in 2024, the same was true last year: in most cases, the reported attacks did not have serious consequences; the most common practical consequence was a reduction in service availability.



FINANCIAL SECTOR: A HIGHLY EXPOSED SECTOR THAT FACES A LARGE NUMBER OF ATTACKS BUT ALSO HAS STRONG RESILIENCE AND RESOURCES

A quarter of respondents in this sector reported having been targeted by a large number of cyberattack attempts (i.e., 101 or more) during the year. This is 9 p.p. higher than the average across all sectors. However, an improvement can be observed compared to 2024, when 33% of organizations reported 101 or more attack attempts. Another positive trend was the increase in attack attempts that did not result in any consequences. In 2025, 50% of all attempts did not result in an incident, representing an improvement of 8 p.p. compared to 2024. **These positive trends were highly likely (75–85%) related to financial institutions' emphasis on cybersecurity, which was reflected in their budgets and, consequently, in their capacities and capabilities.**

Within the financial sector, 81% of respondents considered their cybersecurity budget to be sufficient, which is well above the overall average of 54%. Phishing remained the dominant form of attack. Other social-engineering attacks, such as spear-phishing and fraudulent emails, also remained prevalent. In contrast, vishing declined significantly.



General threats related to the financial sector: cryptocurrency theft

In 2025, there was a growing trend of cryptocurrency thefts by North Korean actors, who use these funds to significantly help finance the North Korean regime's strategic projects, including its nuclear program and ballistic missile development. The North Korean group TraderTraitor is behind the largest cryptocurrency heist to date. In February 2025, the group stole approximately \$1.4 billion (CZK 30 billion) worth of cryptocurrency from the Dubai-based cryptocurrency exchange Bybit. Members of the group exploited vulnerabilities during routine wallet transfers and manipulated transaction processes to divert substantial funds to addresses under their control.

TARGETS OF CYBERATTACKS

INDUSTRY AND ENERGY: A SECTOR SEEING AN INCREASE IN DETECTED CYBERATTACKS, BUT ALSO A DECLINE IN THEIR SUCCESS RATE

In 2025, as in the financial sector, there was a marked increase in the number of cyberattack attempts in the industrial and energy sectors. The number of respondents who reported facing more than 101 attempted attacks increased by 8 p.p. in this sector. At the same time, however, there was a significant decline in the success rate of these attacks, as evidenced by a 9 p.p. decrease in the number of attempts that resulted in a cyber incident. **It can therefore be concluded that in 2025, the trend of increasing cyberattacks on the industrial and energy sectors continued, although these sectors demonstrated greater resilience.**

This may be related to the fact that, according to the majority of respondents (68%), their cybersecurity budgets have increased, even exceeding the expectations set for 2024. **At the same time, this positive trend may also be attributed to the fact that the number of cybersecurity professionals in this sector has increased year-over-year, and approximately 4 p.p. more respondents (currently 87%) reported that their organizations have defined and assigned cybersecurity roles.**

In most cases, the respondents themselves stated that they consider their organization's level of cybersecurity to be sufficient (84% of respondents) and that the level of cybersecurity has improved since last year (95% of respondents).

In 2025, the industrial and energy sectors faced a significantly higher number of cyberattacks, but at the same time were better able to withstand them.

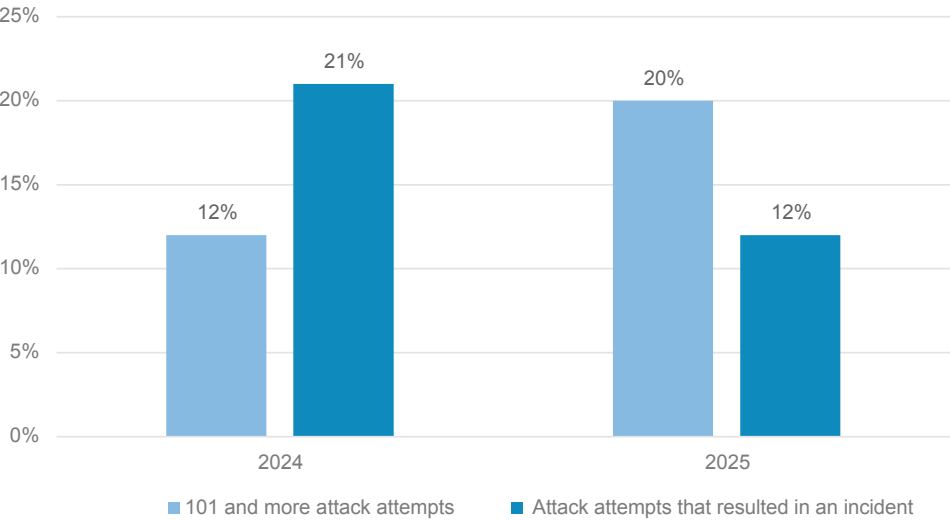


Figure 15: How many attempted attacks did your organization detect last year? How many of those attempts resulted in a cyber incident?

HEALTHCARE: THE NUMBER OF ATTACKS HAS DECLINED, BUT THE SEVERITY OF POTENTIAL CONSEQUENCES REMAINS

The healthcare sector has long been among the most vulnerable, primarily due to attacks with serious consequences—such as ransomware—that can directly impact the delivery of healthcare. In 2025, a ransomware attack led to one such incident in the Czech Republic as well. Overall, several positive trends were observed last year. Although phishing and fraudulent emails continued to dominate, both showed a slight decline compared to the previous year, as did most types of attacks. **Vishing—fraudulent phone calls—saw a significant increase.** These calls were more sophisticated, allowing perpetrators to create a greater sense of urgency among victims. AI tools also contribute to this, as they can be used to create realistic copies of the voices or faces of people known to the victim.

Although phishing and fraudulent emails continue to dominate, we are seeing a decline in these compared to previous years, as is the case in most categories.

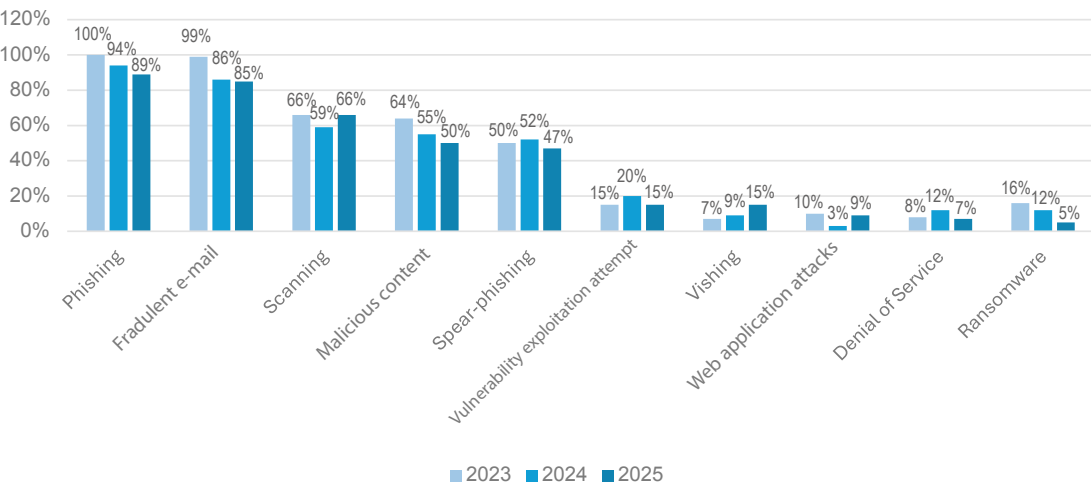


Figure 16: What types of attacks on your organization—or attempts at such attacks—did you experience last year?

Ransomware struck a Czech hospital last year; abroad, it has been proven to have contributed to a patient's death

A ransomware attack on a hospital in Nymburk in early July of last year disrupted the operations of certain departments and services for more than a week. Fortunately, the attack did not jeopardize the provision of acute care and did not put any patients' lives at risk. In London, however, a ransomware attack a month earlier disrupted operations at two hospitals to such an extent that it contributed to the death of a patient. The incident caused delays in more than 10,000 examinations as well as clinical diagnostics, particularly blood tests. According to the hospital, the disruption to laboratory services led to a significant increase in wait times for critical results, which was one of the causes of the aforementioned death.

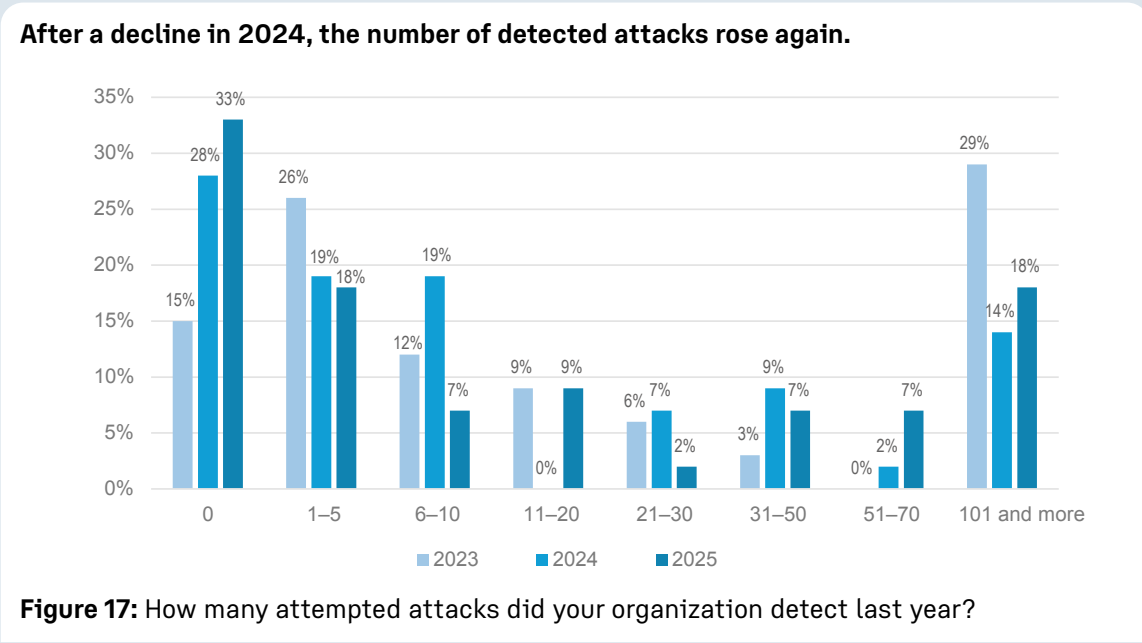
TARGETS OF CYBERATTACKS

EDUCATION SECTOR: THE DECLINE IN THE NUMBER OF DETECTED CYBERATTACKS IN 2024 DID NOT PROVE TO BE A TREND

Following a significantly lower number of recorded attack attempts in 2024, there was another slight increase in 2025. This was primarily due to a higher number of respondents who reported having detected more than 50 attack attempts. The number of respondents who recorded 51–70 attempted attacks increased by 5 p.p., while the number of respondents who reported 101 or more attempted attacks increased by more than 3 p.p. However, these figures are still lower than in 2022 and 2023.

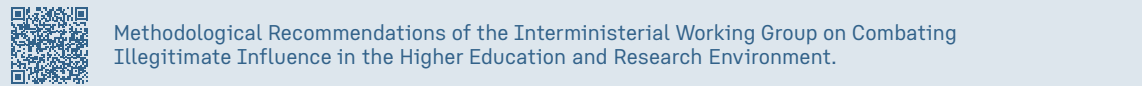
At the same time, fewer attempted attacks resulted in actual cyber incidents in 2025. In this regard, the situation in the education sector was more favorable than in 2024, even though most respondents did not see an increase in their budgets in 2025, despite the expectations they had expressed in 2024.

Expectations for 2026 are less optimistic among most organizations, as only 38% of respondents said they expect an increase in their cybersecurity budget (in 2024, 49% of respondents expected a budget increase in 2025), and 2% of respondents even expect a reduction in their cybersecurity budget in 2026 (no such expectation was reported in 2024).



GENERAL THREATS RELATED TO THE EDUCATION SECTOR: UNDUE INFLUENCE

The influence exerted on individuals or processes through criminal activity, lobbying, or the influence of foreign powers poses a threat not only to academic institutions worldwide but also to those in the Czech Republic. The growing geopolitical significance of research and innovation makes these institutions prime targets, and the principles of openness and internationalization on which they operate generally contribute to their vulnerability.



SENSITIVE AREAS OF RESEARCH AND EDUCATION:

- critical technologies for the EU’s economic security,
- selected fields of research and education,
- selected cooperation with third parties,
- dual-use goods and technologies and military equipment,
- any other areas that a given academic institution decides to include in this category.

The range of potentially useful information and contacts is broad, since even seemingly insignificant bits of information – such as details about an institution’s internal operations – can constitute valuable intelligence.

At the end of 2025, the British newspaper The Telegraph published an extensive investigative report describing the collaboration between leading British universities and their Chinese counterparts, which led to the development of China’s military and arms capabilities. The PRC maintains state oversight of both the private and academic sectors, with many academic institutions directly linked to the defense sector and the military, resulting in a blurring of the lines between the civilian and military spheres. Particularly notable in this regard are the so-called “Seven Sons of National Defense”—seven Chinese universities involved in military research and development. Some of these universities have also collaborated with institutions in the Czech Republic in the past.

TIMELINE OF SELECTED ALERTS AND WARNINGS IN 2025

MAY



The Czech government publicly attributed the cyberattacks to the PRC

In May, the government released a national attribution report on a malicious cyber campaign carried out by the APT31 group, which is linked to China's Ministry of State Security. Since at least 2022, this group has been attacking one of the Ministry of Foreign Affairs' unclassified networks.



Warning regarding a Russian cyber campaign targeting entities supporting Ukraine

In late May, NÚKIB, together with BIS, MI, and other foreign partners, joined in issuing a warning about a long-term cyber campaign waged by APT28, a Russian state-sponsored actor, against logistics and technology companies involved in providing foreign aid to Ukraine.

SEPTEMBER



Warning regarding the threat posed by data transfers and remote administration from the PRC

In September 2025, NÚKIB issued a warning regarding the threat posed by data transfers and remote administration from the PRC. Based on this warning, entities subject to the Cyber Security Act must take this threat into account in their risk analysis and respond to the identified risks by implementing appropriate security measures. The threat is assessed as "High," meaning it is likely to highly likely.

The warning was, to a large extent, groundbreaking. **It does not focus on a single technology but highlights a complex problem and is applicable to all industries, services, and equipment.** Among other things, the warning can also be taken into account in public procurement, and in the event of unacceptable risks, the terms and conditions for deliveries and suppliers can be adjusted.

As is customary, guidelines were issued alongside the warning to explain how to proceed.

JULY



Warning regarding certain DeepSeek products

In July, NÚKIB issued a warning against the use of certain DeepSeek products. These products should not be used on devices with access to critical information infrastructure systems, basic service information systems, and important information systems. Concerns about potential security threats stemmed primarily from data handling practices and the legal and political environment of the PRC, to which DeepSeek is entirely subject.

AUGUST



NÚKIB has joined a joint analysis of the activities of the Chinese state-sponsored actor Salt Typhoon

NÚKIB has joined a joint analysis by U.S. government security agencies and other international partners regarding the Chinese state-sponsored actor Salt Typhoon, which infiltrates networks around the world with the aim of gaining long-term access to them and using them for espionage activities.

DECEMBER



NÚKIB supports the United Kingdom's warning regarding malicious cyber activities by the Chinese companies I-SOON and Integrity Tech

In December, NÚKIB endorsed a statement by partners from the United Kingdom who drew attention to the malicious activities of the Chinese companies Anxun Information Technology and Beijing Integrity Technology operating in cyberspace. These companies are part of a complex ecosystem of private entities in the PRC that, among other things, develop offensive tools for local intelligence and security agencies and, with the knowledge of the Chinese government, carry out offensive cyber operations against foreign targets, including institutions in the Czech Republic.



NÚKIB has joined the warning against attacks by pro-Russian hacktivists

NÚKIB, together with other national partners, has joined the U.S. Federal Bureau of Investigation in issuing a warning about cyberattacks by pro-Russian hacktivist groups targeting critical infrastructure.



THE NEW NATIONAL CYBER SECURITY STRATEGY AND THE DEVELOPMENT OF AN ACTION PLAN TO IMPLEMENT IT FOR THE PERIOD 2026–2030

In September 2025, the government approved an update to the National Cyber Security Strategy (hereinafter “NCSS”). This is the country’s top-level strategic document on cybersecurity, which establishes a unified and coordinated framework focused on:

- the security and resilience of information and communication systems,
- cyber defense,
- cyber diplomacy,
- combating cybercrime and strengthening society’s resilience to threats in cyberspace.

NCSS’s vision is a secure and digitally advanced Czech Republic with resilient infrastructure, an educated and innovative society, and strong international and domestic partnerships. The strategic objectives for realizing this vision are based on a proactive approach to threats, the ability to respond to large-scale crises, and the development of experts. These objectives will be achieved through specific, measurable, achievable, and time-bound tasks outlined in the Action Plan, the preparation and subsequent implementation of which are coordinated by NÚKIB. The Action Plan is scheduled to be submitted to the government in the first half of 2026.

IMPLEMENTATION PLAN FOR THE NATIONAL POLICY ON CRYPTOGRAPHIC PROTECTION OF CLASSIFIED INFORMATION

Following the approval of the National Policy on the Cryptographic Protection of Classified Information (hereinafter “NP CPCI”) at the end of 2024, work on the Implementation Plan proceeded in 2025. The plan contains specific tasks designed to fulfill the objectives of the NP CPCI. The specific wording of the tasks is classified, but they include the following areas: management of the cryptographic protection system, support for domestic cryptographic resources, support for personnel capacities, crisis preparedness, and other areas. The planned timeframe for completing the tasks runs through 2030, with an outlook through 2040 for long-term development topics. The implementation plan was submitted to the State Security Council for approval at the end of 2025.

COORDINATED VULNERABILITY DISCLOSURE

In 2025, work was completed on the National Policy on Coordinated Vulnerability Disclosure (hereinafter “CVD”) and the establishment of related internal processes at NÚKIB (receipt of reports, verification, communication with reporters, etc.). As part of the CVD implementation at NÚKIB, pilot implementation for selected web applications continued, along with an evaluation of the findings. Inter-ministerial consultations were also held to establish a legal and procedural framework so that, once the policy was published, it can be extended to other entities. The CVD was published at the end of 2025; during 2026, there are plans to launch an awareness campaign regarding the implementation of CVD policies in organizations, in conjunction with educational initiatives and methodological support.



THE CYBERLEAGUE PROJECT

The Cyberleague Project aims to create a community of volunteers composed of cybersecurity experts that will operate under the auspices of and in cooperation with NÚKIB. The main objective is to support cybersecurity in the Czech Republic and to provide a platform for a secure, trustworthy, and active community that shares best practices, build expertise, and foster growth and development at both the individual and systemic levels. In 2025, conceptual development of this project continued (establishing rules and processes and consulting with potential members). During the fall, a pilot phase was launched with a smaller group of members, focusing on verifying the project’s practical functionality. The plan is to gradually bring the Cyberleague into full operation during 2026.

NATIONAL LEGISLATIVE FRAMEWORK

Act No. 264/2025, on Cybersecurity

The bill was passed by the Chamber of Deputies in its third reading on April 25, 2025. There were 165 members present; 159 voted in favor of the bill and 0 voted against it. The bill spent a total of nine months in the Chamber of Deputies (from July 25, 2024, to May 13, 2025).

The bill was then referred to the Senate, which approved it by a vote of 66 in favor and 1 against.

Act No. 264/2025, on Cybersecurity, took effect on November 1, 2025, marking the conclusion of nearly four years of preparation for this key piece of legislation. Specifically, the process lasted three years, eight months, and nine days.

Implementation of the Act on Cybersecurity began in November 2025. In 2025, the focus was primarily on the self-identification of obligated entities, their registration, and preparations for implementing security measures for these entities. A complication for NÚKIB in implementing the law was the failure to approve the amendment to the Administrative Procedure Code, which prevented the automated signing of decisions—i.e., sealing—thereby increasing the need for resources to develop new systems and implement automation through alternative means. There are expected to be over 6,000 obligated entities, and a registration decision will need to be issued in each individual case. Without a technical solution, manually signing each decision by an authorized person could take years.

In connection with the Act on Cybersecurity, two government regulations were drafted and submitted to implement the so-called supply chain security review mechanism. This new framework is intended to provide the state with strategic control over the supply chain of the most critical, so-called strategically important services. During the inter-ministerial review process for both regulations, disagreements arose that have not yet been resolved (despite all efforts by NÚKIB), and the draft regulations therefore remain in the inter-ministerial review process.

Without these regulations, the supply chain security verification mechanism contained in the Act on Cybersecurity does not function, as the entities required to comply with it have not been specified. The proposed regulations under consideration are:

- a draft government regulation on essential functions of a specified scope and
- a draft government regulation on regulated services that meet the criteria for strategically important services, and on the components of strategically important services that constitute the necessary scope for ensuring the availability of strategically important services (Regulation on Strategically Important Services).

The year 2025 was also marked by efforts to raise awareness about the Act on Cybersecurity. Staff from the Regulation Department spoke at more than 80 public conferences, workshops, and similar events for the general public. Informational brochures were sent to approximately 35 business associations, organizations, and chambers.

As part of the effort to ensure the smooth implementation of the Act on Cybersecurity, video tutorials—or video lectures—have been created that cover the requirements of the Act on Cybersecurity, individual obligations and security measures, and guidance on using the NÚKIB Portal. These tutorials are published on the NÚKIB Portal and on the NÚKIB YouTube channel, where they have received several thousand views.

REGULATION OF CLOUD COMPUTING USED BY PUBLIC ADMINISTRATION INFORMATION SYSTEMS

In 2025, 41 providers and 12 service offerings were evaluated. Over the entire evaluation period, a total of 187 providers and 32 service offerings were evaluated.

The assessment process is complex. Although 12 new offerings were added to the cloud computing catalog in 2025, NÚKIB had to conduct 63 separate assessments. At the same time, the implementing regulations in this area underwent a comprehensive revision and were significantly simplified in several areas to reduce the administrative burden as much as possible and improve the user experience for those entities subject to the standards.

CRITICAL INFRASTRUCTURE RESILIENCE ACT

Another key piece of legislation with implications for cybersecurity and the operations of NÚKIB is Act No. 266/2025, on the Resilience of Critical Infrastructure Entities and on amendments to related acts (the Critical Infrastructure Act). This Act entered into force in 2025. In addition to providing consultations during the drafting of this Act, NÚKIB was involved in drafting the portion of the government’s implementing regulation that defines the criteria for obligated entities in the field of digital services. In the future, as the guarantor for part of the digital infrastructure sector, it will also confirm the registration of critical infrastructure entities in this sector.

EU LEGISLATIVE FRAMEWORK

THE CYBERSECURITY ACT AND ITS AMENDMENT

The [Cybersecurity Act](#) (hereinafter “CSA”) establishes a voluntary cyber security certification system for information and communication technology (hereinafter “ICT”) products, services, and processes, as well as for managed security services. Thanks to a unified European cybersecurity certification framework, manufacturers can demonstrate the security level of their products in a manner recognized throughout the EU, thereby strengthening the trust of both customers and business partners. CSA certification is thus primarily a tool for improving trust and transparency. The regulation has been in effect since 2019, and the first certificates under the European Cybersecurity Certification Scheme (hereinafter the “EUCC”) may be issued starting in February 2025. A revision of this regulation is currently underway at the European level; the draft was presented in January 2026. NÚKIB has been actively involved in submitting both its own and joint comments on the CSA revision.

As part of this agenda, NÚKIB prepared to carry out these tasks; in particular, it adopted an internal directive setting out all the key procedures of a national cybersecurity certification authority, consulted with the Czech Accreditation Institute on the introduction of an accreditation service in accordance with the EUCC (including the approval of assessment experts, revisions to internal documentation, etc.) and also began comprehensive preparations for the peer review process (a mutual evaluation of compliance with requirements by the European Commission and other Member States, scheduled for October 2026).

CYBER RESILIENCE ACT

The [Cyber Resilience Act](#) (hereinafter the “CRA”) is horizontal legislation establishing cybersecurity requirements for all products with digital elements placed on the EU market. The goal is to ensure security throughout the entire product lifecycle—from design through manufacturing to updates. The CRA requires manufacturers to actively manage vulnerabilities, report incidents, and undergo a conformity assessment process.

In November 2025, an important implementing act was negotiated and adopted that specifies the technical definitions of significant and critical products under the CRA; NÚKIB was actively involved in these negotiations.

Information on both regulations, including supporting materials,



is available on the NÚKIB Portal.



EU CRISIS MANAGEMENT

In June 2025, the Council of the EU adopted a new framework for cybersecurity crisis management in the form of a Council Recommendation on an EU Plan for Addressing Cybersecurity Crises—the so-called [Cyber Blueprint](#)—which updates and replaces the Commission’s original 2017 recommendation. The Cyber Blueprint establishes a framework for a coordinated EU response to large-scale cyber incidents, including a clear division of roles among relevant cybersecurity actors at the EU level, coordination with other EU crisis management mechanisms, and cooperation with NATO.

SIMPLIFICATION PACKAGE

In November 2025, the European Commission published the so-called [Digital Simplification Package](#), which includes both legislative and non-legislative initiatives in the areas of data regulations, personal data protection, and cybersecurity. The package includes the Digital Omnibus, which, among other things, proposes the establishment of a unified interface for reporting incidents, the so-called Single-Entry Point. NÚKIB has been actively involved in the discussions on this matter from the outset.

NETWORK CODE

The [Network Code](#) is a set of technical rules that harmonize cybersecurity in the operation and management of cross-border energy networks in the EU, with the aim of establishing common minimum requirements for planning, monitoring, reporting, and crisis management through binding requirements for system operators, generators, and other market participants. This standard introduces binding cybersecurity requirements, including risk management and incident response. As part of this agenda, NÚKIB focused on preparing for implementation and collaborating with other relevant authorities to ensure the smooth implementation of the requirements.

DIGITAL OPERATIONAL RESILIENCE ACT

[Digital Operational Resilience](#) (hereinafter “DORA”) is an EU regulation that establishes a unified framework for digital operational resilience in the financial sector with the aim of strengthening cybersecurity and the ability of financial institutions (banks, insurance companies, investment firms, crypto-asset providers, etc.) to withstand cyberattacks, respond to them effectively, and recover quickly. It sets out rules for ICT risk management, incident reporting, resilience testing, and oversight of critical third parties (IT service providers). Since some entities subject to DORA are also subject to the Act on Cybersecurity, coordination and clarification regarding the implementation of both regulations were necessary with the Czech National Bank, which oversees DORA.

SUPERVISORY ACTIVITIES

During 2025, NÚKIB conducted a total of 22 inspections and audits in accordance with Act No. 181/2014, on Cybersecurity, and its implementing Decree No. 82/2018, on Security Measures, Cybersecurity Incidents, Reactive Measures, Requirements for Submissions in the Field of Cybersecurity, and Data Destruction, as amended.

In addition to its own audit activities, NÚKIB continued to focus on providing methodological support to regulated entities, which consisted primarily of responding to technical inquiries on an ongoing basis, preparing and publishing support materials, and conducting audits of selected entities.

In connection with updates to the relevant legislation, NÚKIB is simultaneously and gradually issuing a set of methodological materials intended for regulated entities. The goal is to facilitate the interpretation of new and amended obligations, standardize implementation practices, and provide practical support for the implementation of the required security measures.

COOPERATION BETWEEN NÚKIB AND OTHER SUPERVISORY AUTHORITIES ON INSPECTIONS IN 2025

In 2025, NÚKIB continued to strengthen its cooperation with other regulatory authorities. NÚKIB participated in the inspection activities of the State Office for Nuclear Safety as an invited participant. At the same time, meetings were held with representatives of the Czech National Bank to define the next steps for mutual cooperation regarding the impact of new regulations on the banking sector and the field of cybersecurity.

MOST IMPORTANT SHORTCOMINGS IDENTIFIED DURING AUDITS IN 2025

The information security management system does not cover all assets that are relevant from a cybersecurity perspective.

Risk analysis is not conducted systematically enough, nor to the required extent.

Cybersecurity supplier management processes exhibit significant shortcomings.

Business continuity management is not addressed adequately or is completely neglected, leaving organizations unprepared to handle the impacts of cybersecurity incidents.

Multi-factor authentication mechanisms are not implemented, and authentication passwords are not sufficiently strong.

Measures to protect against malicious code and the ability to detect cybersecurity incidents on internal networks are insufficient.

Technical equipment that is no longer supported by the manufacturer is in use and poses an increased security risk.

The cryptographic measures in use do not meet current requirements for cryptographic strength.

Backups are not sufficiently tested or adequately protected.

CYBERSECURITY EXERCISES

In 2025, NÚKIB focused its efforts in the area of exercises on conceptual work related to the preparation and drafting of the National Cybersecurity Exercise Concept. **The document's vision is to build a robust, flexible, and sustainable long-term exercise system that responds to current and future challenges in the field of cybersecurity.** This vision will be realized through two pillars, building capabilities and capacities for conducting exercises, and systematizing and deepening cooperation in the area of exercises.

In 2025, exercises with an international scope were also held, including the traditional Locked Shields exercise organized by the NATO Cooperative Cyber Defense Center of Excellence in Tallinn, Estonia, which took place in May. In December, the international cybersecurity exercise Cyber Coalition, also organized under the auspices of NATO, took place. NÚKIB also participated in an Alliance exercise for crisis management authorities. For its allies, NÚKIB prepared and organized an exercise focused on the capability to provide remote support during cyber incidents (VCISC – Virtual Cyber Incident Support Capability). The goal was to test allies' readiness to provide mutual assistance through the VCISC mechanism in the event of serious cyber incidents.

PREVENTION, AWARENESS-RAISING AND EDUCATION

During 2025, a new NCSS and a draft Action Plan were prepared, incorporating themes related to awareness-raising, education, and prevention for the years 2026–2030. A key change from the previous period is the requirement for significantly broader involvement of public sector organizations in the implementation of prevention and education activities, including support for regional initiatives, school programs, and targeted campaigns for various population groups.



The NÚKIB educational portal offers awareness courses for schools, the healthcare sector, government agencies, and the general public. NÚKIB creates and sponsors a course focused on the basics of cybersecurity, Dávej kyber, and a course for cybersecurity managers, Šéfuj kyber.



Last year, NÚKIB joined efforts to warn the public about fraudulent phone calls in which an unknown attacker posed as an employee of a trusted institution and, under the pretext that an account had been blocked and money needed to be transferred to a reserve account, attempted to defraud victims of their money.

INTERNATIONAL COOPERATION

NATO COOPERATION

During 2025, NÚKIB initiated and led discussions among national stakeholders focused on preparations for the implementation of the NATO Integrated Cyber Defense Center, whose establishment was announced in 2024. NÚKIB was also involved in an internal assessment of NATO's operations in the area of cybersecurity and defense.

NEW STRATEGIC RELATIONSHIPS

In March 2025, as part of the Prague Cyber Security Conference 2025 (hereinafter the "PCSC"), a memorandum of cooperation was signed between NÚKIB and the Ukrainian State Service of Special Communications and Information Protection of Ukraine. The memorandum focuses primarily on cooperation in the exchange of information and the sharing of experiences and best practices in areas such as incident response, threat analysis, and enhancing the cybersecurity of critical infrastructure. **Following this memorandum, NÚKIB organized a workshop where, together with other international partners, it shared its experiences with the implementation of the NIS 2 Directive requirements, EU cooperation in the area of cybersecurity incident response, and cybersecurity crisis management.**



In May, NÚKIB contributed to several Australian technical documents focusing on the fundamentals of modern resilient infrastructure, the security of border network elements, and the use of Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms.



In September, NÚKIB endorsed the document *A Shared Vision of Software Bill of Materials (SBOM) for Cybersecurity*, which was issued by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA), together with other international partners. The document aims to encourage wider use of this tool in practice.

RELATIONS WITH THE USA

The year 2025 was marked primarily by the inauguration of the new U.S. administration and expectations regarding the continuation of close cooperation with the U.S. and European partners. A NÚKIB delegation held a series of meetings with representatives of U.S. security institutions, including the White House National Security Council and the House Select Committee on Strategic Competition between the U.S. and China, during which both sides reaffirmed their commitment to continue working closely together and exchanging experiences and information in the field of countering cyber threats. NÚKIB representatives attended the RSA Conference, the world's leading cybersecurity conference, and, alongside top officials from the U.S. administration and international partners, spoke at the International Cyber Security Forum. The good relations between the two countries were further reinforced by a visit by a delegation from the Czech Ministry of Foreign Affairs to the U.S. toward the end of the year.

DEVELOPMENT COOPERATION AND CYBER CAPACITY BUILDING

In 2025, NÚKIB participated in numerous development projects and shared its expertise primarily with partners in the Western Balkans and the Indo-Pacific region, but also, to a lesser extent, in Africa and Asia. **However, the Western Balkans remain the priority region for the allocation of development aid.** In its development activities, NÚKIB continues to cooperate with international organizations (particularly NATO and the EU) and key like-minded countries, including the U.S. and Estonia. At the same time, however, it actively participates in the Ministry of Foreign Affairs' CyberVAC development projects; in 2025, these primarily involved projects in Jordan and Bhutan.

EU COOPERATION

ENISA SUPPORT ACTION

Activities continued in the ENISA Support Action project, through which selected entities were provided with free penetration testing services, cyber exercises, and assistance with risk analysis.

SUPPLY CHAIN TOOLBOX

Within the Cooperation Group established by the NIS 2 Directive, work was completed on a set of measures to enhance the security of the ICT supply chain (the so-called ICT Supply Chain Security Toolbox). The Toolbox was published on February 13, 2026, along with two coordinated risk assessments at the EU level (connected and autonomous vehicles and detection equipment) that follow its structure.

CONFERENCES

PRAGUE CYBER SECURITY CONFERENCE 2025

NÚKIB hosted the sixth annual international PCSC, which once again brought together government officials, experts, and private-sector representatives from dozens of countries around the world. The main topics, under the theme "Invisible Frontlines," included the invisible frontlines of cyber conflicts, strengthening the resilience of critical infrastructure, protecting energy and telecommunications networks, the impacts of artificial intelligence (hereinafter "AI"), and the importance of international cooperation in combating cyber threats.

CONFERENCE CYBER_CON 2025

The 11th annual CYBER_CON 2025 conference, organized by NÚKIB in collaboration with partners CZ. NIC, NIX.CZ, CESNET, and others, attracted nearly 800 participants to the Brno Exhibition Center. On September 17 and 18, 2025, technical and legal specialists, academics, managers, and students gathered to discuss current challenges and opportunities in the field of cybersecurity. The conference program was structured around the NCSS and the Act on Cybersecurity.

EUROPEAN CERTIFICATIONS CONFERENCE

On November 26, 2025, NÚKIB organized the second annual European Certification Conference. This year's event focused on upcoming legislative changes that will significantly impact manufacturers throughout the EU. The main topic of the conference was CSA, though updates on CRA were also presented. Conference participants had the opportunity to discuss the expected impacts of CRA, conformity assessment processes, and other aspects of placing products with digital elements on the EU internal market. A total of 112 participants registered for the conference, and 71 of them attended in person.

GOVERNMENT CERT ACTIVITIES

In 2025, in addition to its routine forensic work, the Government CERT continued to develop its active on-site assistance to affected entities, specifically while addressing the consequences of cybersecurity incidents directly within their infrastructure. Furthermore, these capabilities were applied in a proactive network threat hunting service. There are also plans to further develop this service and combine it with other proactive approaches to improve the cyber resilience of regulated entities.

NÚKIB PORTAL

Intensive development of the NÚKIB Portal took place throughout 2024 and 2025. Since November 1, 2025, it has become a key tool for implementing the Act on Cybersecurity and the NIS 2 Directive and serves as a single point of contact for regulated entities to fulfill their legal obligations to NÚKIB. At the same time, the Portal can be used to report cyber incidents and securely share information about vulnerabilities and threats. In the public section of the Portal, organizations can find methodologies, guides, and support materials needed to fulfill their new obligations.

The Portal was designed to significantly reduce the administrative burden for both NÚKIB and regulated entities. **In November 2025, it won second place in the national category of the Egovernment The Best 2025 competition.** This competition annually recognizes the most successful public administration digitization projects in the Czech Republic. Throughout 2025, the portal received more than 252,000 visitors.

ACTIVE VULNERABILITY MONITORING



A new active vulnerability monitoring service was launched, addressing an average of approximately 20 vulnerabilities per day. Alerts are posted on X on an ongoing basis, with about twenty issued each month. For vulnerabilities with a high impact on the Czech Republic, alerts were issued directly on the NÚKIB Portal, and in cases of targeted impacts, affected parties were specifically notified. In 2025, over 140 such alerts were issued.

PENETRATION TESTING

A total of 10 entities were tested. Compared to previous years, there was an increase in demand for comprehensive penetration tests, which included physical testing, Wi-Fi infrastructure, and phishing campaigns. Compared to the previous year, the number of penetration tests conducted rose from 23 to 36, representing a year-over-year increase of approximately 56%.

In 2025, an advanced phishing infrastructure called “Phishing 2.0” was developed, enabling the bypassing of two-factor authentication. At the same time, the process of selecting and purchasing a new vulnerability scanner was underway; in accordance with the Act on Cybersecurity, this scanner will enable automated scans of a larger number of entities.

Consultations and testing of the PENTEREP tool are conducted regularly in collaboration with Brno University of Technology (VUT).

To further develop technical capabilities, the GOAD laboratory infrastructure was deployed to enhance the practical knowledge of the team and, where appropriate, other CERT teams.



OUTLOOK: CYBERSECURITY TRENDS IN THE CZECH REPUBLIC FOR 2026 AND 2027

OUTLOOK: CYBERSECURITY TRENDS IN THE CZECH REPUBLIC FOR 2026 AND 2027

THE THREAT OF MISUSE OF COMMUNICATION PLATFORMS FOR THE DISSEMINATION OF HARMFUL CONTENT AND CYBER ESPIONAGE

Throughout 2025, several spear-phishing campaigns were recorded in Europe that exploited the Signal messaging platform to distribute spyware. Communication via Signal is generally considered secure thanks to its end-to-end encryption; however, encryption itself does not guarantee the authenticity of conversation participants. Nevertheless, it is popular among journalists and government employees, creating an opportunity to obtain relevant sensitive information. Although no similar attacks were recorded in the Czech Republic last year, the possibility that they will occur in the future cannot be ruled out (40-50%).

Some of the recorded attacks targeted members of the Ukrainian armed forces, with a significant portion of these incidents attributed to actors linked to Russia or sponsored by the Russian state. Several of these attacks were directly attributed to the Russian actor APT28 by the Ukrainian CERT and private cybersecurity companies. It can be concluded that this was one of the group's most frequently used modus operandi over the past year.

This type of attack is not limited to the Signal platform; over the past year, similar campaigns have been observed on platforms such as WhatsApp, but for the reasons mentioned above, targeting via Signal poses a specific threat to national security. The U.S. Cybersecurity and Infrastructure Security Agency also issued warnings about the spread of spyware via communication platforms in the second half of 2025.

AI: A TECHNOLOGY THAT IS STABILIZING, BUT WHOSE FUNDING IS DIFFICULT TO SUSTAIN

In 2025, AI had become a mature technology that was beginning to show signs of stagnation. The release of the fifth version of ChatGPT did not bring dramatic improvements to the service's capabilities, as previous versions had, and competing services also failed to deliver a significant breakthrough that would set a new industry standard. The rivalry between the West and PRC in the field of AI continued to play out at the geopolitical level, but it had less of an impact on direct competition in, for example, Western mobile app markets, where—after a brief period of interest in Chinese AI models—Western apps once again dominated, and Chinese services shifted their focus to the domestic market.

However, the year 2026 could bring major turning points in the field of AI. **Current AI based on large language models** (hereinafter “LLM”) **is still not profitable, even four years after its commercial launch.** AI requires energy-intensive computations on advanced hardware, and its operation is not profitable under current conditions. OpenAI CEO Sam Altman admitted that the company loses money on every user, including those who pay for the highest-tier premium subscription costing more than 4,000 crowns per month. Companies that develop and operate AI offset these losses either through other sources of revenue or with investor funds. Currently, however, there are warning signals that further investment in the AI sector may stall,

precisely because of its current lack of profitability and the absence of a clear plan for future effective monetization. Moreover, the current influx of investment relies not only on potential future profitability but also, to a large extent, on the promise of further breakthroughs in the field of AI, leading to the development of artificial general intelligence (AGI) capable of surpassing humans. At present, however, we are seeing a rise in skepticism regarding whether LLM-based AI can even achieve this state.

In 2026, therefore, a scenario in which investment declines is likely (55–70%). The situation surrounding OpenAI—as the leader and pioneer of current AI services, though one that is largely dependent on investors—is particularly crucial. OpenAI is already facing financial difficulties, which it is addressing, for example, by scaling back its service portfolio—such as by discontinuing the Sora video generator—or by inserting ads into ChatGPT. It is likely (55–70%) that this situation will continue to worsen in the coming years and could even lead to the company's collapse. The collapse of OpenAI would highly likely (75–85%) have a domino effect on the rest of the AI sector and would undermine confidence in the future of the entire AI industry.¹ **An outflow of investor funds could lead to significant restrictions on or price increases for current AI services. This situation could subsequently lead to a strengthening of the positions of Chinese AI services, such as MinMax or DeepSeek.** Although these companies are almost certainly (90–100%) also operating at a loss, their investment sources are different and tied to the Chinese regime. The regime can therefore continue to finance them, precisely with the aim of filling the void left by Western models.

Czech companies are therefore likely (55–70%) to face the risk of either an outage, a decline in quality, or a significant price increase for Western AI models over the next two years. Consequently, they may be forced under pressure to switch to models of Chinese origin, with the risks associated with them (e.g., data processing and storage in the PRC, with the risk of industrial espionage). It is therefore recommended that companies adopt AI technologies sparingly, while retaining the ability to revert to their original processes.

¹ Although companies like Meta or Google have their own sources of revenue (primarily from advertising), they are publicly traded, and their stock prices would likely be significantly weakened as a result.

ANNEX 1: EVALUATION OF THE FULFILMENT OF THE OBJECTIVES OF THE NATIONAL RESEARCH AND DEVELOPMENT PLAN ON CYBERSECURITY AND INFORMATION SECURITY 2025

BUILDING A NATIONAL COORDINATION CENTER

In 2025, NÚKIB continued to provide services as the [National Coordination Center](#) in accordance with Regulation (EU) No. 2021/887 of the European Parliament and of the Council. In this context, NÚKIB organized several webinars and training sessions focusing on current calls for proposals under The Digital Europe program, the services of the National Coordination Center, and the process for registering with the Competence Community under the Act on Cybersecurity.

NÚKIB continued to build its information infrastructure, provide consulting services on accessing funding from EU framework programs, and disseminate research and development results within the Czech Republic. Efforts to strengthen ties between the academic, private, and public sectors were carried out primarily through regular meetings of the Cyber Research and Innovation in Security group [CYRIS](#), which brings together approximately 150 members of the research and development community. NÚKIB also publishes a regular newsletter focused on the latest developments in cybersecurity research and development.

As part of the PROPED initiative to support economic and scientific diplomacy, NÚKIB carried out three international scientific missions with the aim of deepening cooperation in the fields of cybersecurity, cryptographic protection, and space technologies.

SUPPORT FOR RESEARCH AND DEVELOPMENT PROJECTS

As an application guarantor, NÚKIB has supported more than twenty research and development projects funded through public competitive programs (such as the Technology Agency of the Czech Republic or the Ministry of the Interior's security research program) with the aim of increasing the practical applicability of research and development results. NÚKIB has also participated in international research consortia—one example is the QARC project, funded through the Horizon Europe programme, which aims to accelerate the transition to quantum-secure cryptography through close collaboration between academia, industry, and the public sector.

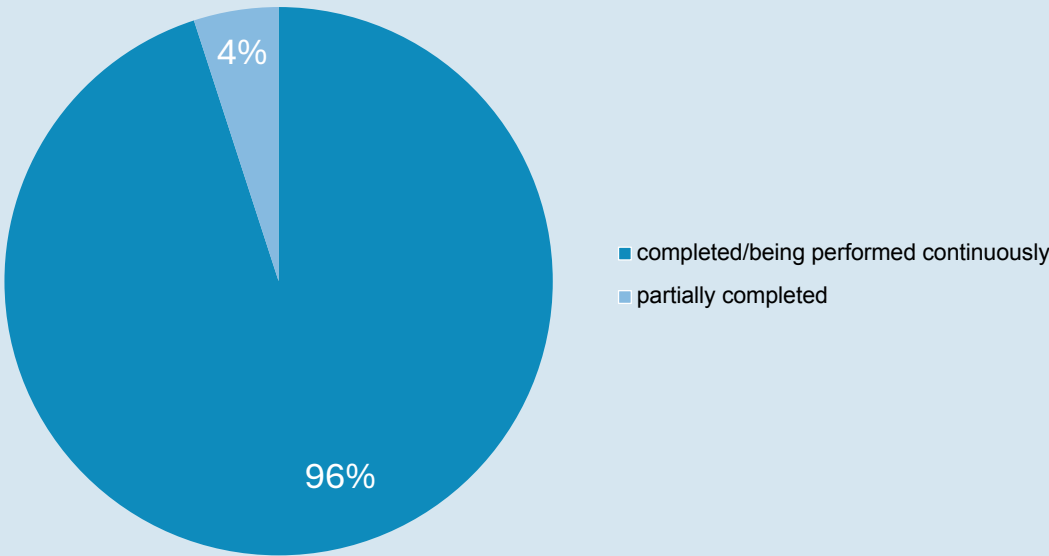
ACTIVITIES AT THE EU LEVEL

At the EU level, NÚKIB continued to contribute to the preparation of a number of strategic documents that are key to the functioning of the European Cybersecurity Competence Center and to the substantive focus of the Digital Europe program.

ANNEX 2: IMPLEMENTATION OF THE ACTION PLAN FOR THE NATIONAL CYBER SECURITY STRATEGY OF THE CZECH REPUBLIC FOR 2021-2025

In 2025, the implementation of the Action Plan for the National Cybersecurity Strategy for 2021-2025 (hereinafter the "Action Plan") was evaluated for the fifth time. Given the introduction of the new NCSS and the expiration of the Action Plan, this is also its final evaluation.

In total, 83 tasks were evaluated for the year 2025. Of this number, 3 tasks were only partially completed; all other tasks were evaluated as completed or in progress. The task completion rate was therefore 96%, which is the highest completion rate for the entire 2021-2025 strategic period.



Complex tasks, in particular, were only partially completed. Their completion depends on external circumstances beyond the control of those responsible for them, and they are often repeatedly carried over to subsequent years. An example is Task No. 13: "Develop a methodology for strategic communication among relevant entities at the national level for responding to cyber incidents, attacks, and other threats," which was originally scheduled for completion in 2022 but has not yet been completed due to a lack of capacity on the part of the responsible entities.

Despite a consistently high success rate in task completion, a small proportion of inadequately completed tasks has appeared in every year's evaluation of the Action Plan to date. In addition to the aforementioned capacity constraints, a common reason for inadequate completion is the reprioritization of the agendas entrusted to the lead agency. Lessons learned from tasks that were not successfully completed are being incorporated into the preparation of the new Action Plan for 2026-2030, whose tasks also build on some of the unfinished tasks from the previous period.

ANNEX 3: IMPLEMENTING REGULATIONS FOR THE NEW ACT ON CYBERSECURITY

The law is implemented through a total of 10 implementing regulations, of which 7 are decrees, 2 are government regulations, and 1 is an implementing regulation of the European Commission. With the exception of the government regulations, all of these implementing regulations had already been adopted by 2025. Specifically, these are:

- Decree No. 408/2025, on Regulated Services, which defines the identification criteria for obligated entities,
- Decree No. 409/2025, on Security Measures for Providers of Regulated Services Under the Enhanced Obligations Regime, which defines security measures for entities subject to the enhanced obligations regime,
- Decree No. 410/2025, on Security Measures for Providers of Regulated Services Under the Lower-Level Obligation Regime, which defines security measures for obligated entities under the lower-level regime,
- Decree No. 334/2025, on the Authority's Portal and Requirements for Selected Actions, which defines how communication with the regulator will take place and what information must be reported,
- Decree No. 411/2025, on the Security Levels of Public Administration Information Systems (hereinafter "PAIS"), which relates to the regulation of the use of cloud computing services in PAIS and, for these purposes, establishes criteria for classifying PAIS into security levels based on their impact,
- Decree No. 412/2025, on Security Rules for Public Administration Bodies Using the Services of Cloud Computing Providers, which defines the security rules that must be implemented by public administration bodies that use cloud computing services to ensure the operation of their PAIS,
- Decree No. 505/2025, on Certain Requirements for Inclusion in the Cloud Computing Catalog, which defines the security measures that a cloud computing provider and service must meet in order to provide cloud services to PAIS,
- Commission Implementing Regulation (EU) 2024/2690 of October 17, 2024, laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements for measures to manage cybersecurity risks and further specifying the cases in which an incident is considered significant with regard to DNS operators, top-level domain registries, cloud computing service providers, data center service providers, content delivery network providers, managed service providers, managed security service providers, online marketplace providers, Internet search engines and social media platform services, and trust service providers; it also sets out the specific regulatory requirements for digital service providers.

ABOUT NÚKIB

NÚKIB is the central administrative authority for cybersecurity, including the protection of classified information in the area of information and communication systems and cryptographic protection. It is also responsible for matters related to the publicly regulated service within the Galileo satellite system. NÚKIB was established on August 1, 2017, pursuant to Act No. 205/2017, which amended Act No. 181/2014, on Cybersecurity and on amendments to related laws (the Act on Cybersecurity).

For more information about NÚKIB, visit our website www.nukib.gov.cz or follow news about cybersecurity in the Czech Republic on our social media [X](#), [LinkedIn](#), [Facebook](#) and [Instagram](#). Recordings of some events that NÚKIB organizes or that its representatives attend can be found on NÚKIB's [YouTube](#) channel.

O NÚKIB

NÚKIB PLAYS A CRITICAL ROLE IN SAFEGUARDING THE CYBERSECURITY OF THE CZECH REPUBLIC AND ITS CITIZENS THROUGH VARIOUS FUNCTIONS:

providing timely, clear, and relevant information to entities involved in critical information infrastructure, basic service operators, and public administration bodies;

ensuring the security of classified information within information and communication systems, including the application of cryptographic protection;

managing cyber incidents by leveraging its expertise and access to information for effective incident management;

providing methodological support and education, and raising awareness on cybersecurity topics;

organizing training sessions and cyber exercises on both national and international levels;

engaging in cybersecurity research and development to advance the field;

offering technical assistance and services such as security scans, penetration testing and vulnerability assessments;

monitoring compliance with the Act on Cybersecurity by regulated entities;

representing the Czech Republic in international cybersecurity bodies and organizations;

conducting analyses of cybersecurity trends to anticipate and respond to emerging threats;

assessing cybersecurity risks and implementing corrective and preventive measures as needed;

preparing national security standards, laws and sub-legal norms related to cybersecurity;

cooperating with the public, private, and academic sectors on both national and international levels.

