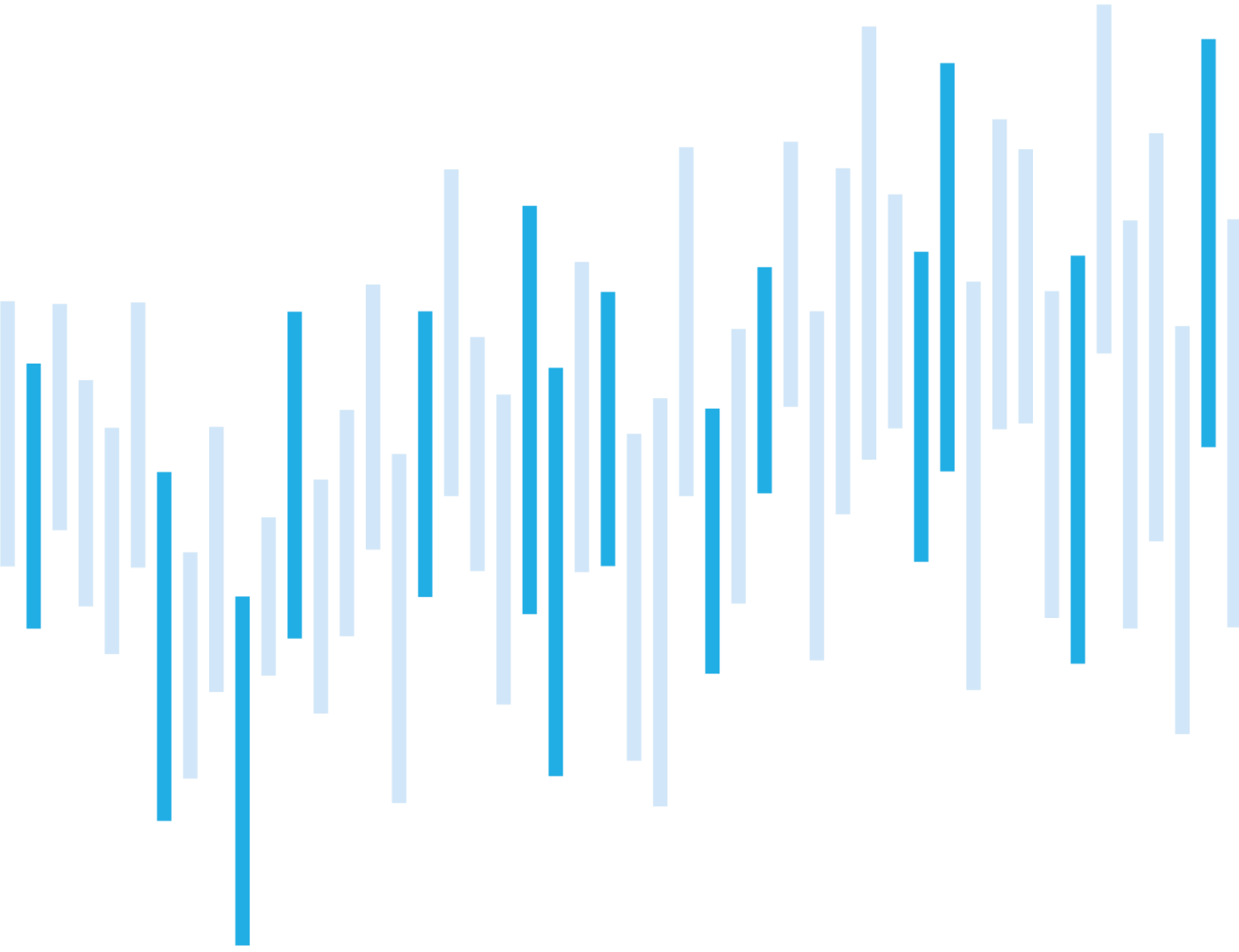
CYBER SECURITY INCIDENTS FROM THE NÚKIB'S PERSPECTIVE

DECEMBER 2024



National Cyber and Information Security Agency

Summary of the month

The last month of 2024 brought 16 incidents, so it was a below-average month in terms of numbers. Similar to November, NÚKIB recorded only minor incidents.

Availability remains the main category with 10 recorded incidents. Most of them were DDoS attacks. The number of ransomware attacks dropped to only one recorded incident at the end of the year.

In the Focus on a Trend chapter, we recap 2024 in terms of incidents, trends and other significant events. The total annual number of recorded incidents climbed to 268, six more than in 2023. The slight difference from the number reported in previous monthly summaries is explained in the chapter below.

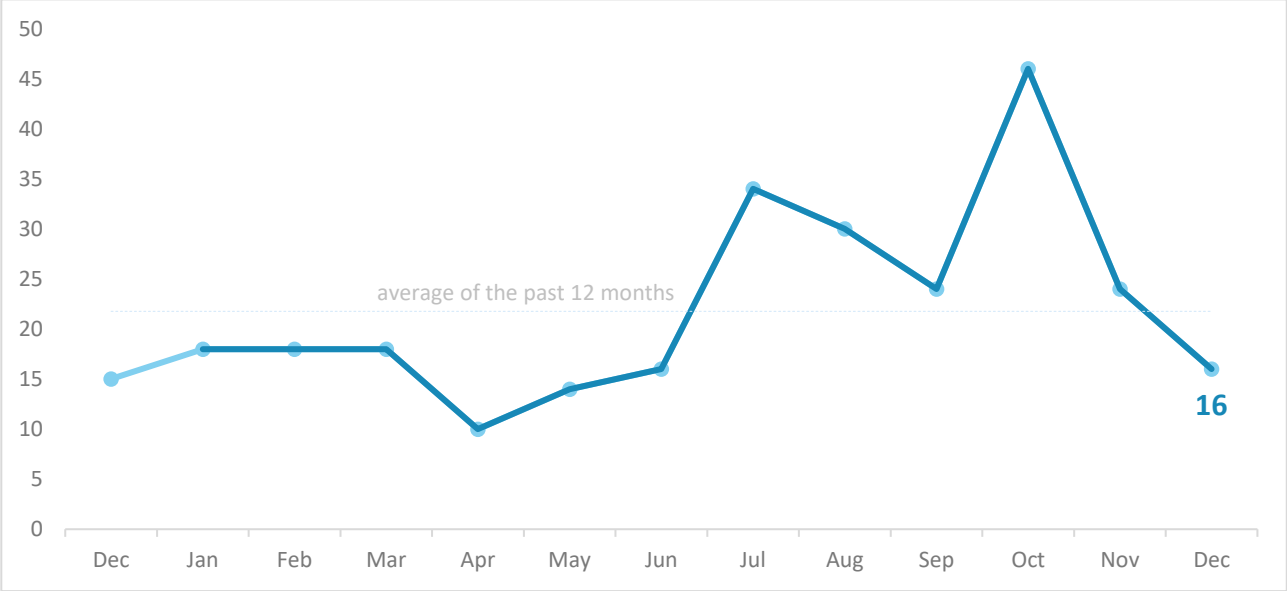
Table of contents

The following report summarises the events of the month. The data, information and conclusions contained herein are primarily based on cyber incidents reported to NÚKIB. Where the report contains information from open sources in some sections, the origin of this information is always indicated.

Comments and suggestions for improving the report can be sent to komunikace@nukib.gov.cz.

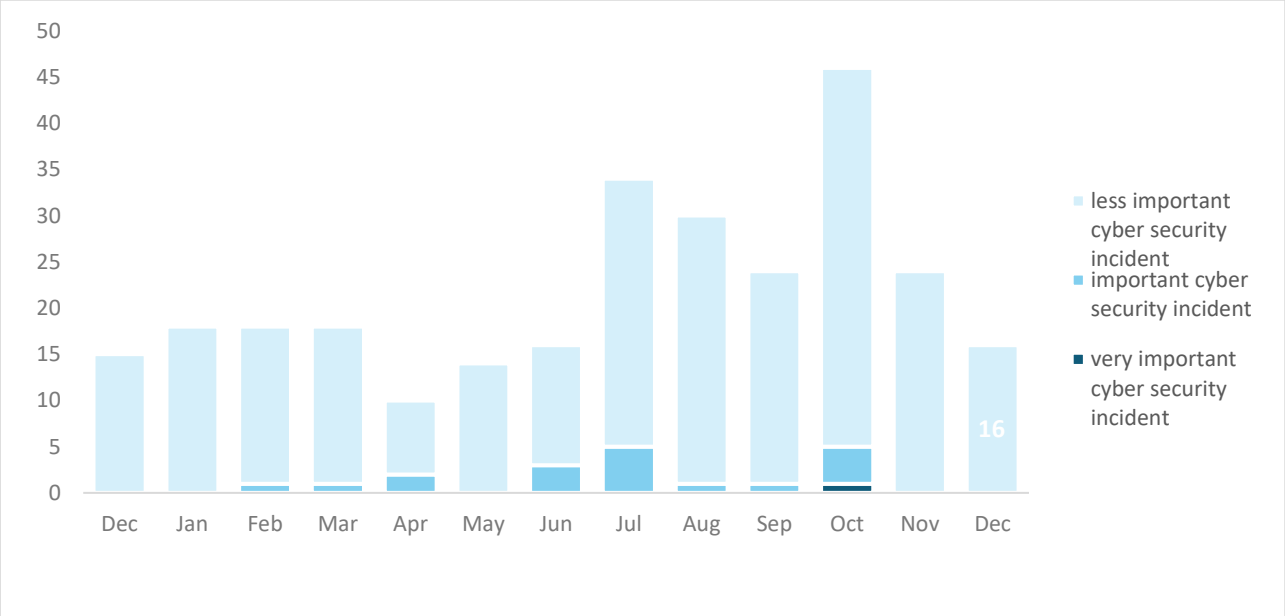
Number of cyber security incidents reported to NÚKIB

In December, NÚKIB recorded 16 cyber incidents. The end of the year was therefore below average.



Severity of the handled cyber security incidents[1]

The severity of recorded incidents remained low in December, with all December incidents classified as minor.



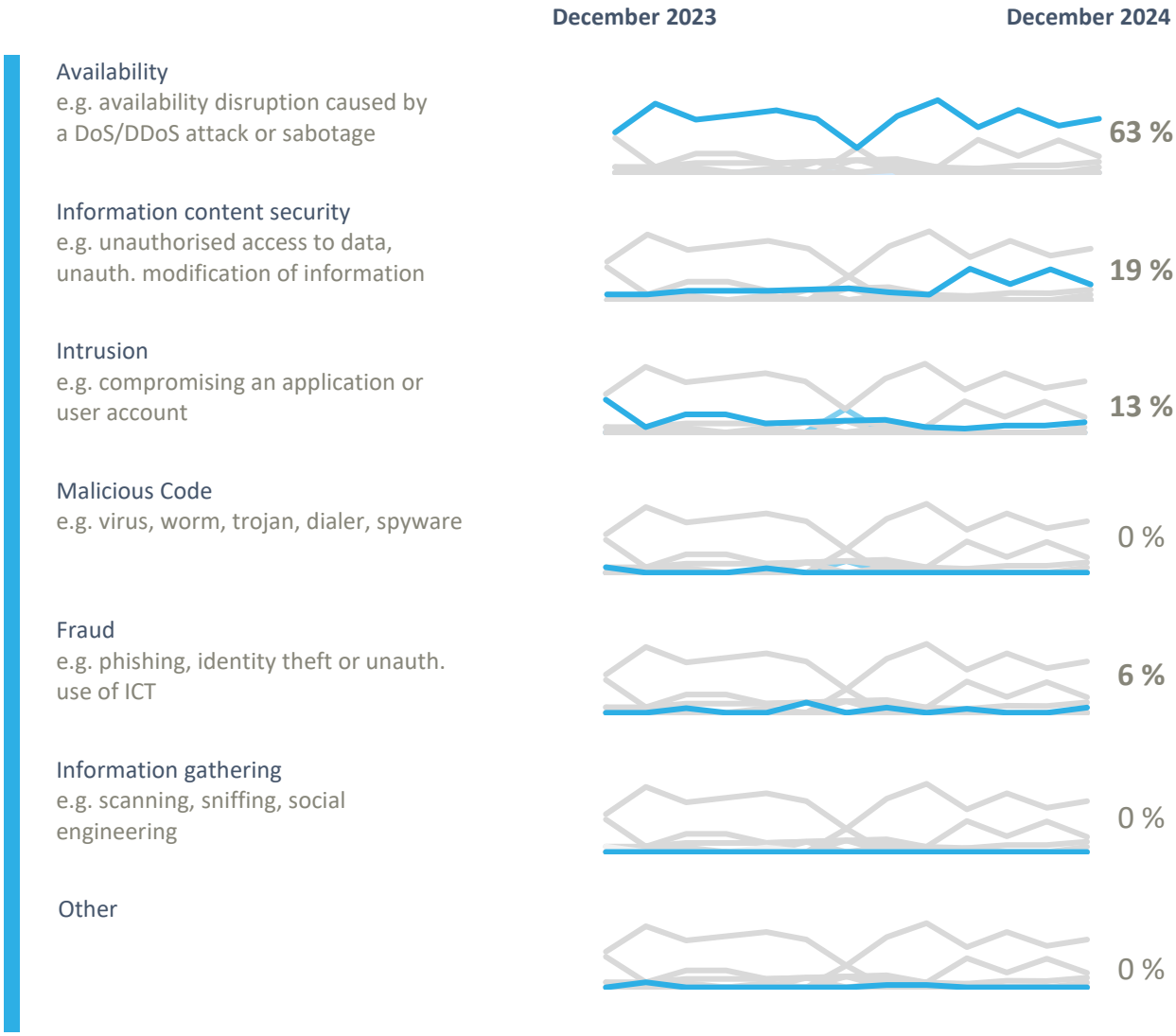
[1] NÚKIB determines the severity of cyber incidents on the basis of Decree No. 82/2018 Coll. and its internal methodology.

Classification of the incidents reported to NÚKIB [2]

As in previous months, Availability remains the most frequent category of incidents. In December, it consisted of seven DDoS attacks and three service outages due to technical failures.

NÚKIB also dealt with incidents in three categories:

- Three incidents fell into the Information Security category, one of which was a ransomware attack, specifically the Ransomhub group. The other two cases involved unauthorised access to systems.
- Within the category of Intrusion, NÚKIB recorded two incidents involving the compromise of a server and the hacking of one user account.
- The final category recorded was Fraud, where a false invoice was sent via spear-phishing and paid by the victim. The total damage was roughly 40 000 EUR.



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

November trends in cyber security from the NÚKIB's perspective [3]

Phishing, spear-phishing and social engineering

In December, NÚKIB recorded one incident involving spear-phishing. Specifically, it involved sending a false invoice under a fake customer identity.

Malware

In December, as in the previous months, there were continuous activities regarding malware analysis in connection with some previously recorded incidents.

Vulnerabilities

In December, NÚKIB continued to publish vulnerabilities via the social network X.

Ransomware

Only one ransomware attack was recorded in December.

Attacks on availability

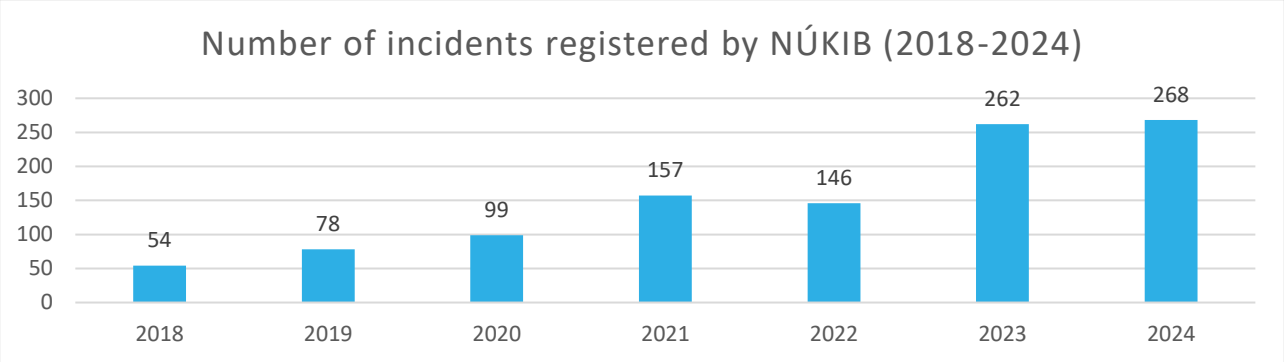
During the month of December, NÚKIB recorded seven DDoS attacks.

[3] The development illustrated by the arrow is evaluated in relation to the previous month.

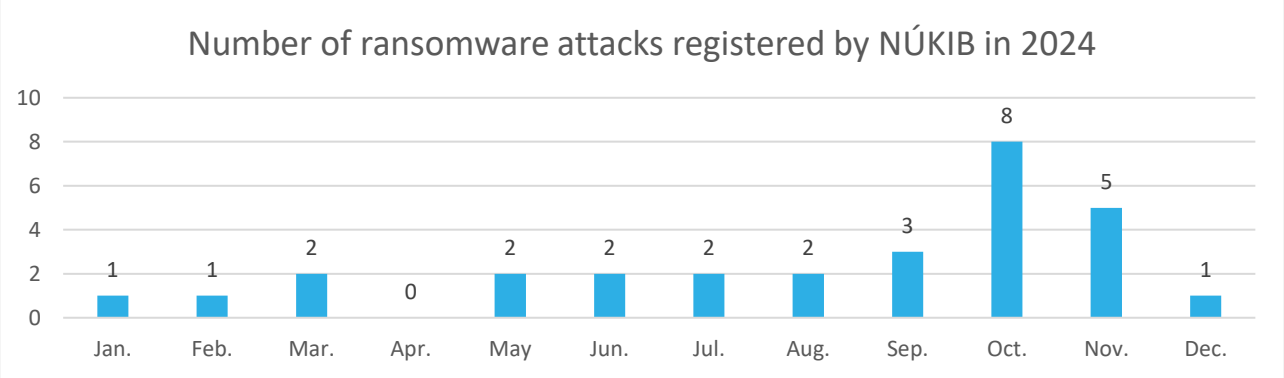
Focus on a trend: Recapitulation of incidents in 2024 from the NÚKIB's perspective

In 2024, NÚKIB recorded a total of 268 cyber security incidents, which is the highest number recorded to date. Compared to 2023, when 262 incidents were registered, this is only a slight increase. The composition of incidents is very similar to last year, with DDoS attacks by Russian-speaking hacktivists accounting for the largest share (43%). The malicious activity of actors from the Middle East region was also partially recorded. However, these malicious activities did not result in significant impacts beyond short-term outages of the affected sites.

The difference in the final number, severity or categories compared to previous monthly summaries is due to the regular annual evaluation of the entire inventory and the associated re-categorisation. Another reason could be the retrospective inclusion of incidents that were reported or detected later.



The threat of ransomware attacks also persisted throughout the year, with NÚKIB typically recording single digit incidents each month, while the actual number of attacks in the Czech Republic, beyond NÚKIB's visibility is almost certainly (90–100 %) higher. Although ransomware attacks made up less than 11 % of all recorded incidents in 2024, their impact underscores their severity. In addition to exfiltration of sensitive citizen or client data, they can lead to data encryption, often leading to the temporary suspension of production or service availability. These consequences inevitably result in reputational and financial damage. In autumn, NÚKIB recorded more than double the average number of such attacks. However, this was likely not a coordinated campaign but rather an increase in activity from multiple attackers.



A specific event with global impact was the failure of CrowdStrike's EDR software, which, due to a faulty update, caused widespread system outages across multiple sectors in July, leading to the unavailability of various services. Domestically, the impact was less severe than in other Western countries, but NÚKIB still recorded a total of nine related incidents.

Probability terms used

Probability terms and expressions of their percentage values:

Term	Probability
Almost certain	90–100 %
Highly likely	75–85 %
Likely	55–70 %
Realistic probability	40–50 %
Unlikely	20–35 %
Highly unlikely	0–15 %

Traffic Light Protocol

must be used in accordance with the Traffic Light Protocol (TLP) methodology, available at https://www.first.org/tlp/. Each piece of information is marked with a flag that defines its usage conditions. The following flags indicate the nature of the information and its usage conditions:

Colour	Conditions of use
TLP:RED	Strictly for individual recipients only – no further disclosure permitted. TLP:RED is used when sharing information could pose significant risks to privacy, reputation, or operations, making further action impractical. Recipients must not share TLP:RED information with anyone. For example, in a meeting, TLP:RED information may only be shared with those physically present.
TLP:AMBER+STRICT	Restricts sharing to the organization only.
TLP:AMBER	Limited disclosure: Recipients may only share this information on a need-to-know basis within their organization and with its clients. TLP:AMBER is used when information requires collaboration to take effective action but poses risks to privacy, reputation, or operations if shared beyond the involved organizations. Recipients may share TLP:AMBER information within their organization and with its clients, but only on a need-to-know basis to safeguard operations and prevent further harm.
TLP:GREEN	Limited disclosure: Recipients may share this information within their community. TLP:GREEN is used when information helps raise awareness within a broader community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, provided it is not distributed through publicly accessible channels. TLP:GREEN information must not be shared beyond the defined community.
TLP:CLEA	Recipients may share this information publicly without restriction. TLP:CLEAR is used when information poses minimal or no foreseeable risk of misuse and complies with applicable rules for public release. TLP:CLEAR information may be freely shared, subject to standard copyright rules.