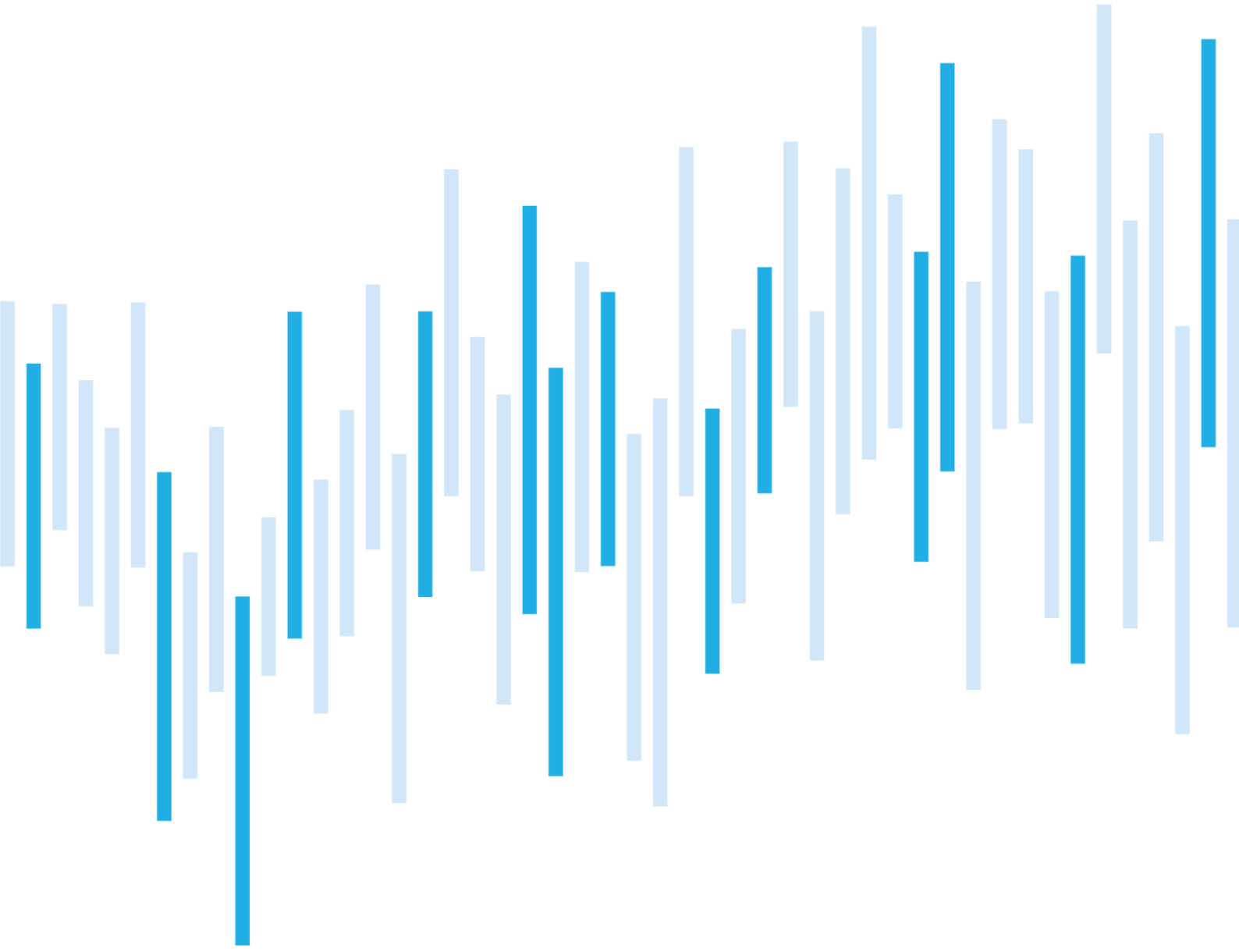
CYBER SECURITY INCIDENTS FROM THE NÚKIB'S PERSPECTIVE

NOVEMBER 2024



National Cyber and Information Security Agency

Summary of the month

In November, NÚKIB registered 24 cyber security incidents, all of which were classified as less important. Compared to the record-breaking October, the number of incidents was close to the average values of the past year.

Availability continues to be the main category. In November, however, it was mostly made up of incidents related to technical failures, with only 5 DDoS attacks recorded.

In the Focus on the Threat chapter, we focus this time on the persistent threat of ransomware attacks. In recent months, the frequency of these attacks has been above average, and although the information available does not indicate an active campaign, but rather increased activity by individual attackers, their attacks can cause significant financial damage to victims.

Table of content

Number of cyber security incidents reported to NÚKIB

Severity of the handled cyber security incidents

Classification of incidents reported to NÚKIB

November trends in cyber security from NÚKIB's perspective

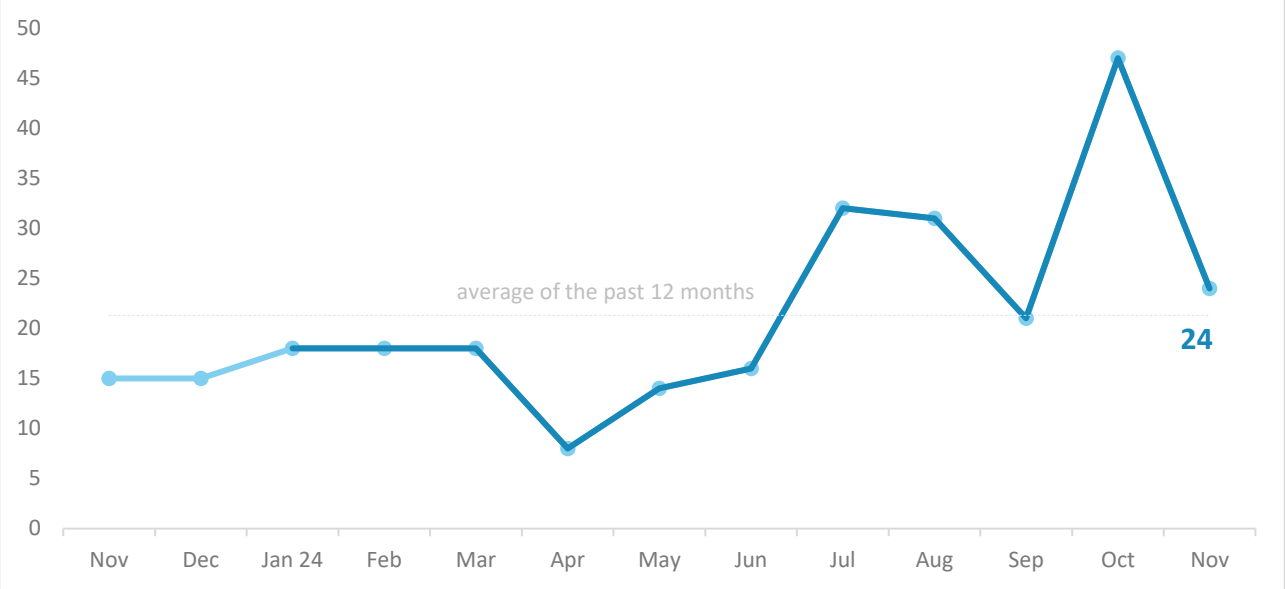
Focus on a threat: Ransomware remains a persistent threat

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. If the report contains information from open sources in some sections, the origin of this information is always stated.

You can send comments and suggestions for improving the report to the address komunikace@nukib.gov.cz

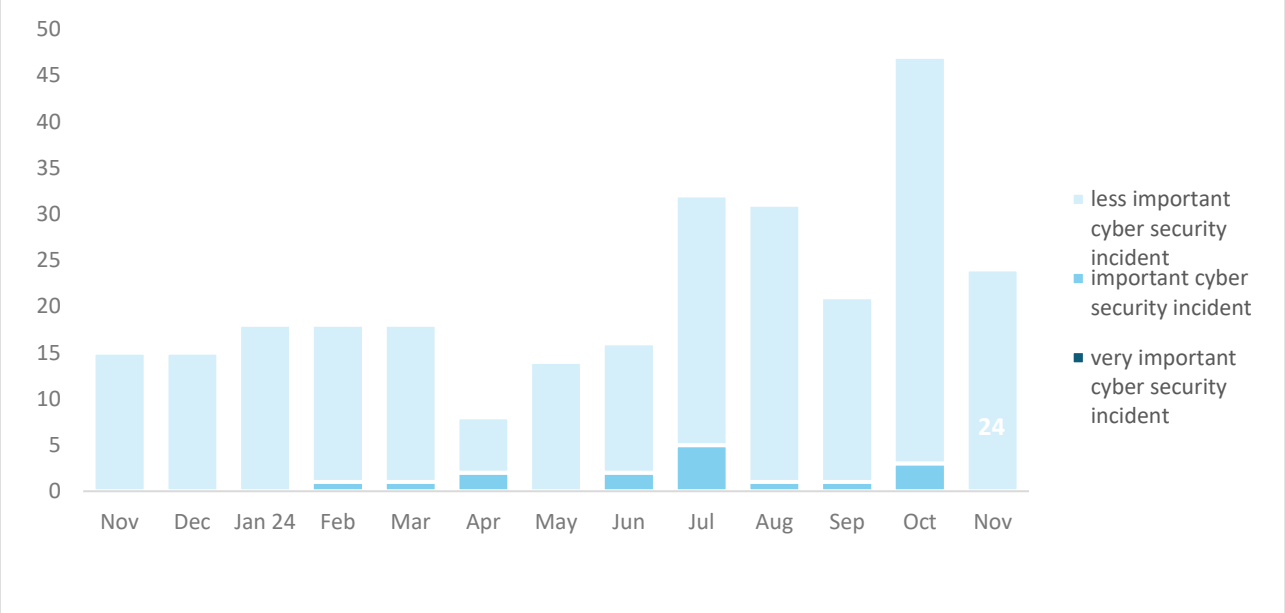
Number of cyber security incidents reported to NÚKIB

In November, NÚKIB recorded 24 cyber incidents. After a record-breaking October, this is a return to the average values for the past year.



Severity of the handled cyber security incidents[1]

The severity of recorded incidents remains low, with all incidents in November classified as less important.



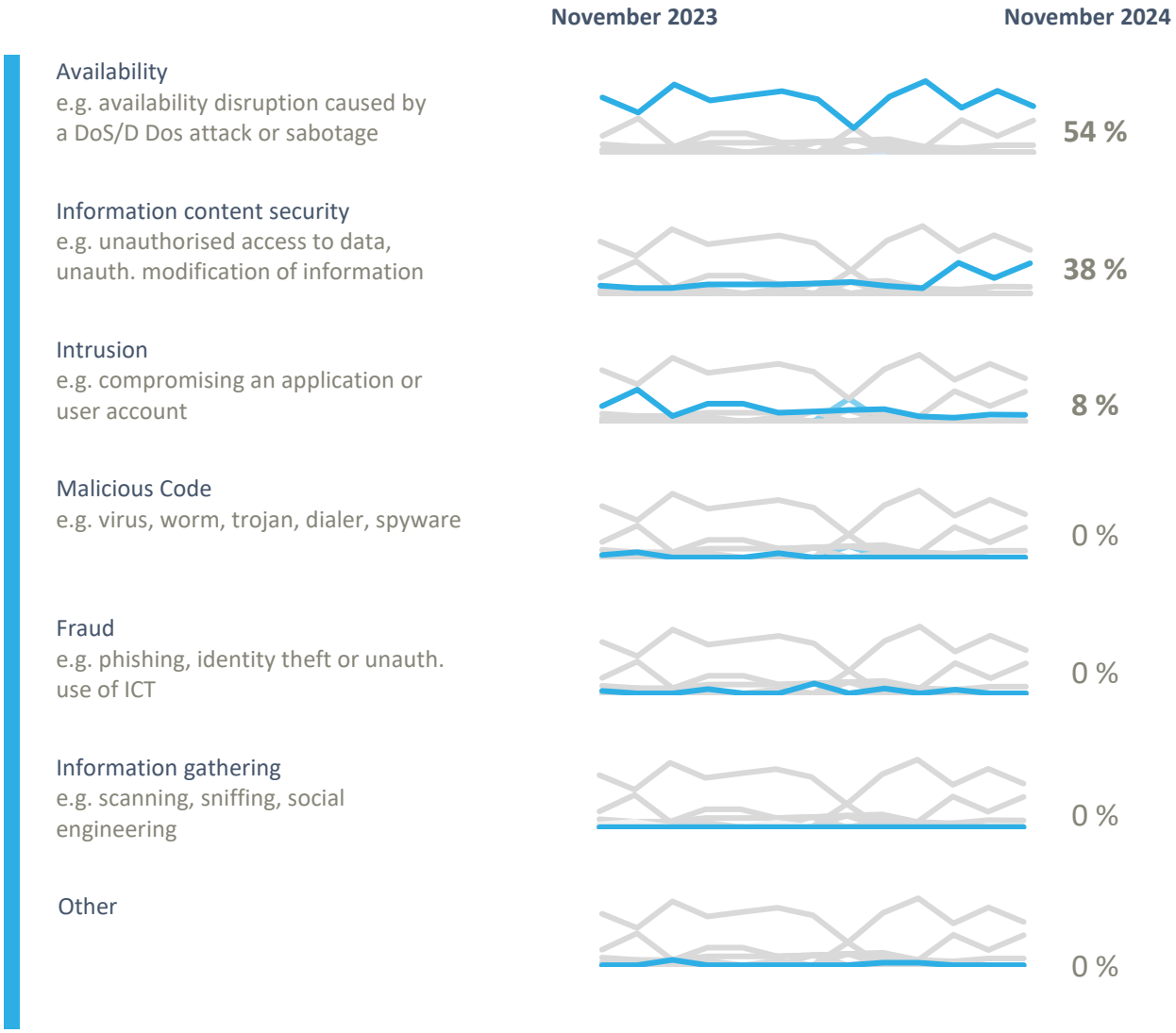
[1] NÚKIB determines the severity of cyber incidents on the basis of Decree No. 82/2018 Coll. and its internal methodology.

Classification of the incidents reported to NÚKIB [2]

As in previous months, Availability remains the most frequent category of incidents. However, compared to October, the majority of incidents in this category were technical glitches or misconfigurations. There were only five DDoS attacks recorded in November.

NÚKIB also handled incidents in two other categories:

- Nine incidents fell into the Information Security category, five of which were ransomware attacks and the remaining cases were data leaks or unauthorized access to systems.
- Within the category of Intrusion, NÚKIB recorded two incidents involving the hacking of user accounts. One case involved compromise of user accounts and subsequent spamming. The second incident involved two students' unauthorized attempts to change their classmates' grades within the school system using a stolen password.



[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 November, NÚKIB recorded one incident involving phishing. A health sector institution was affected, and the email accounts of two of its employees were compromised. The attacker sent spam from the compromised accounts.

Malware

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

Vulnerabilities

During November, NÚKIB continued to publish vulnerabilities through the social network X.

Ransomware

In November, five cases of ransomware attacks were recorded. For more information, see Focus on the threat chapter.

Attacks on availability

During November, NÚKIB recorded 5 DDoS attacks. After a record October, the frequency of these attacks has dropped significantly.

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

Focus on a threat: Ransomware attacks remain a persistent threat

The past quarter has shown that ransomware attacks continue to be a significant threat, not only in terms of severity but also in terms of frequency. In fact, the period saw above-average levels of ransomware-related incidents.

In October, NÚKIB even registered a record number of ransomware attacks targeting both public and private entities. While the number of this type of incidents is normally in the lower units, NÚKIB registered eight incidents during October and five in November. According to NÚKIB findings so far, this was not a coordinated campaign, but only individual attacks by a number of different ransomware gangs. Within the registered ransomware attacks, several types of ransomware were recorded. Smaller units were recorded for Ransom Inc and Akira ransomware, which are also currently among the most active across Europe.

NÚKIB has also recorded successful compromises affecting the operation of the entity for a number of victims. **An inadequate or non-existent backup system often leads to victims dealing with the incident for days or weeks, causing significant financial damage, not to mention the reputational risks arising from the possible disclosure of sensitive internal or client information by the attackers.**

In the context of this threat, NÚKIB has previously issued a supporting analysis, Ransomware: Recommendations for Mitigation, Prevention and Response, which summarises the key recommended actions. AFCEA and NAKIT also contributed to the document.

In addition to providing methodological support to Czech entities, NÚKIB is also addressing this threat internationally. In October, representatives of NÚKIB, Pavel Štěpáník, Deputy Director of the Strategic Agendas and Cooperation Section, and Berta Jarošová, Cyber Attachée for Cooperation with the USA and Canada, represented the Czech Republic at the fourth edition of the International Counter Ransomware Summit. During the Summit, high-level representatives from a total of 68 countries and organizations, including Interpol, discussed the increase in ransomware attacks against strategic institutions and entities, strengthening information sharing or actively disrupting the activities of ransomware groups. The summit was also an opportunity to discuss other strategic topics such as the use of artificial intelligence to combat cyber threats, strengthening resilience or supply chain security in the energy sector.

This year's summit reaffirmed that ransomware remains one of the key national security threats facing states across continents. As in previous years, the Summit adopted both a general joint statement and a declaration calling for responsible behaviour by states in cyberspace and the use of all available tools and resources to combat ransomware. The Czech Republic joined both declarations.

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

The information provided shall be used in accordance with the Traffic Light Protocol methodology (available at the website https://ww.first.org/tlp/). The information is marked with a flag, which sets out conditions for the use of the information. The following flags are specified that indicate the nature of the information and the conditions for its use:

Colour	Conditions of use
TLP:RED	For the eyes and ears of individual recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.
TLP:AMBER+STRICT	Restricts sharing to the organization only.
TLP:AMBER	Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.
TLP:GREEN	Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defence community.
TLP:CLEAR	Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.