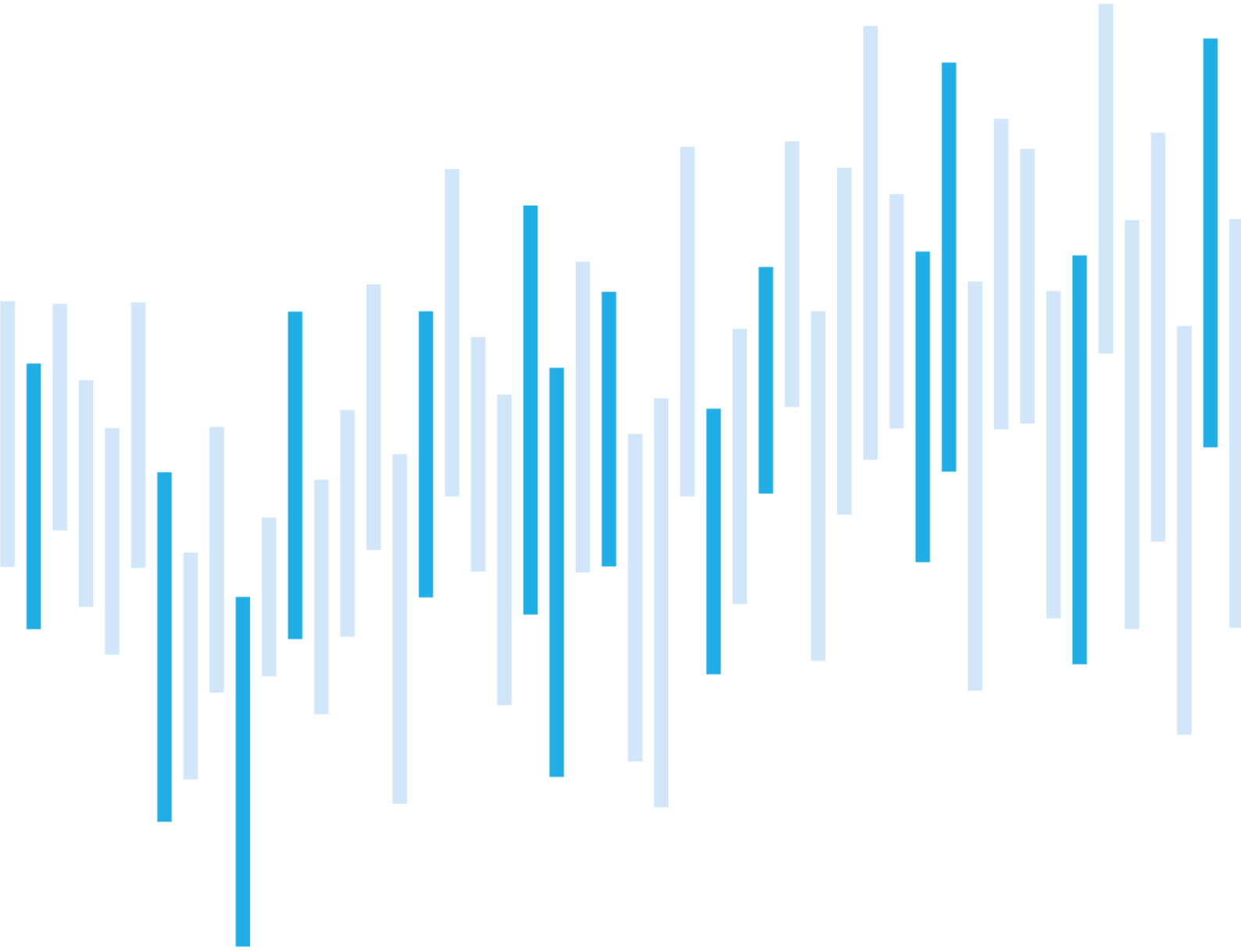
CYBER SECURITY INCIDENTS FROM NÚKIB'S PERSPECTIVE

MARCH 2025



National Cyber and Information Security Agency

Summary of the month

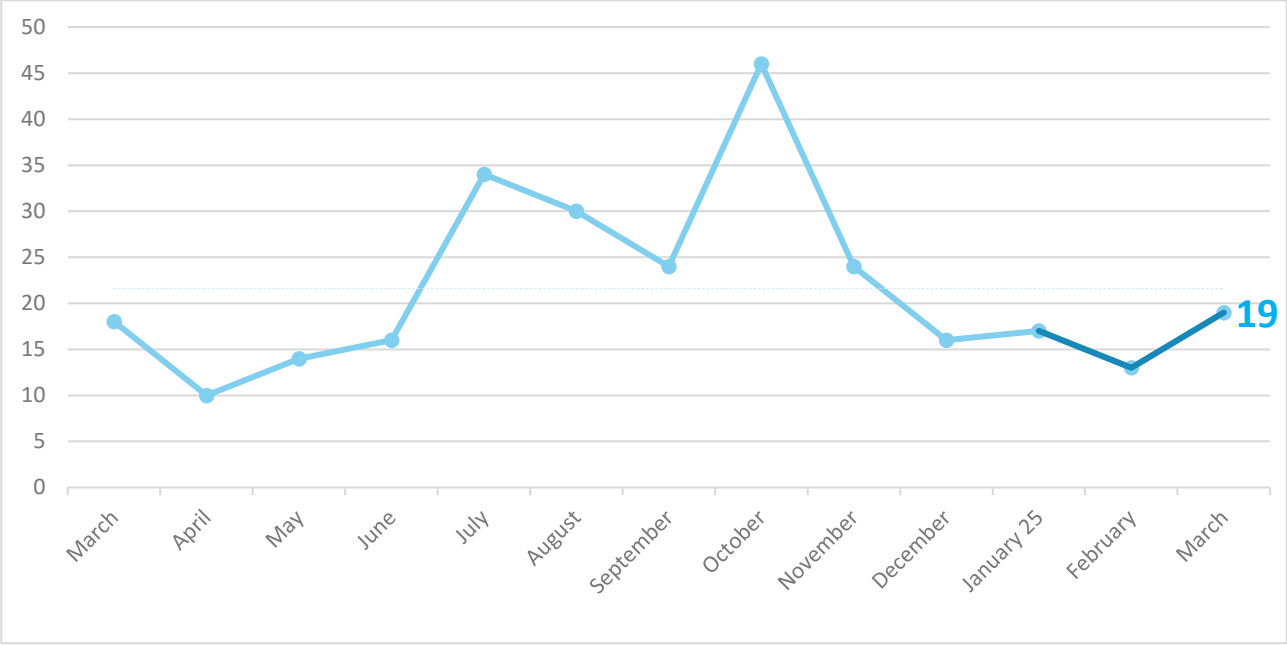
During March, NÚKIB registered 19 cybersecurity incidents, marking a slight increase compared to February. The most represented category was Information Security (7), followed by Intrusion (4). The traditionally most numerous category, Availability, accounted for only three incidents in March, all of which were DDoS attacks. Additionally, NÚKIB recorded two incidents in the Malicious Code category, two cases of Fraud and one Attempted Intrusion.

The Information Security category included six ransomware attacks, and one case of data exfiltration followed by extortion. This reflects a continued trend of increasing ransomware incidents. However, as seen at the end of last year, these attacks seem to be carried out by different actors rather than as a part of a coordinated campaign.

In terms of severity, one ransomware attack – targeting a municipal government – was classified as significant. Although the attack was successful, the affected data was restored from backups. Another ransomware incident targeting the systems of the Fire Brigade of the Czech Republic, specifically in Královéhradecký and Zlín regions, was classified as very significant. The remaining 17 incidents were assessed as less significant.

Five cyber events were also recorded in March. Four of these were unsuccessful phishing or spear-phishing attempts, primarily aimed at financial gain or the collection of login credentials. The fifth event concerns the Oracle data leak, which was highlighted on the NÚKIB portal.

Number of cyber security incidents reported to NÚKIB



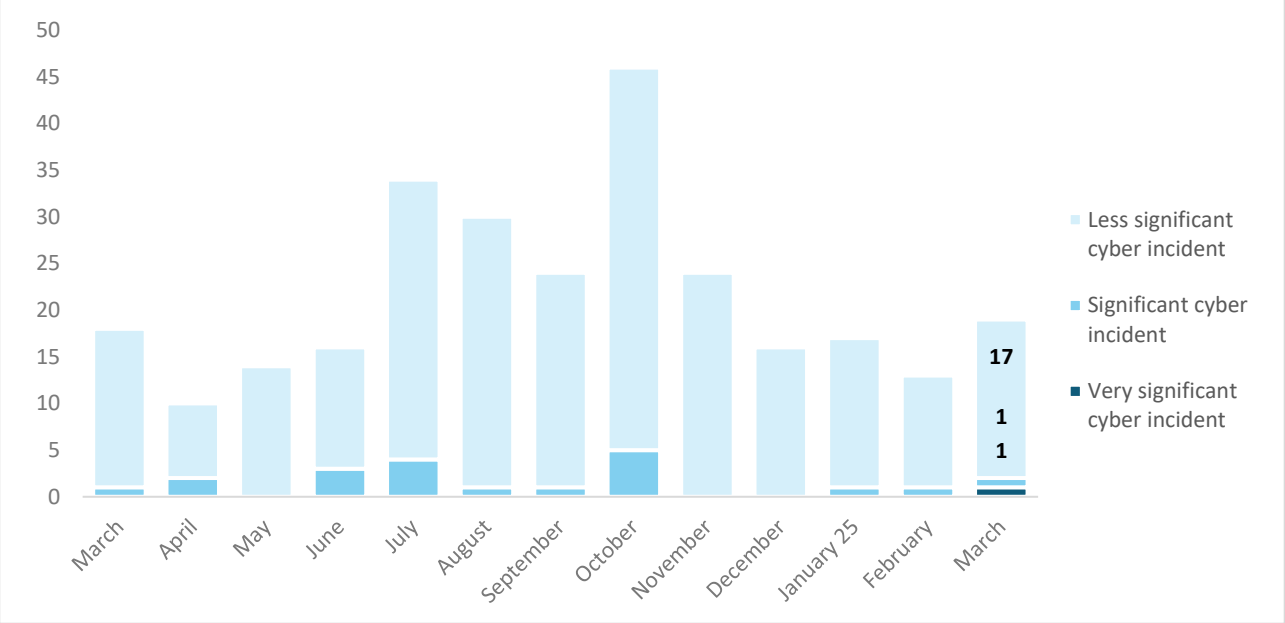
This report provides a summary of the month's events. The data, information and conclusions presented herein are primarily based on cyber incidents reported to NÚKIB. Where information from open sources is used, the source is always clearly indicated.

Please note that some values in the incident log may be subject to retrospective updates. As a result, historical data presented in graphs may change over time.

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

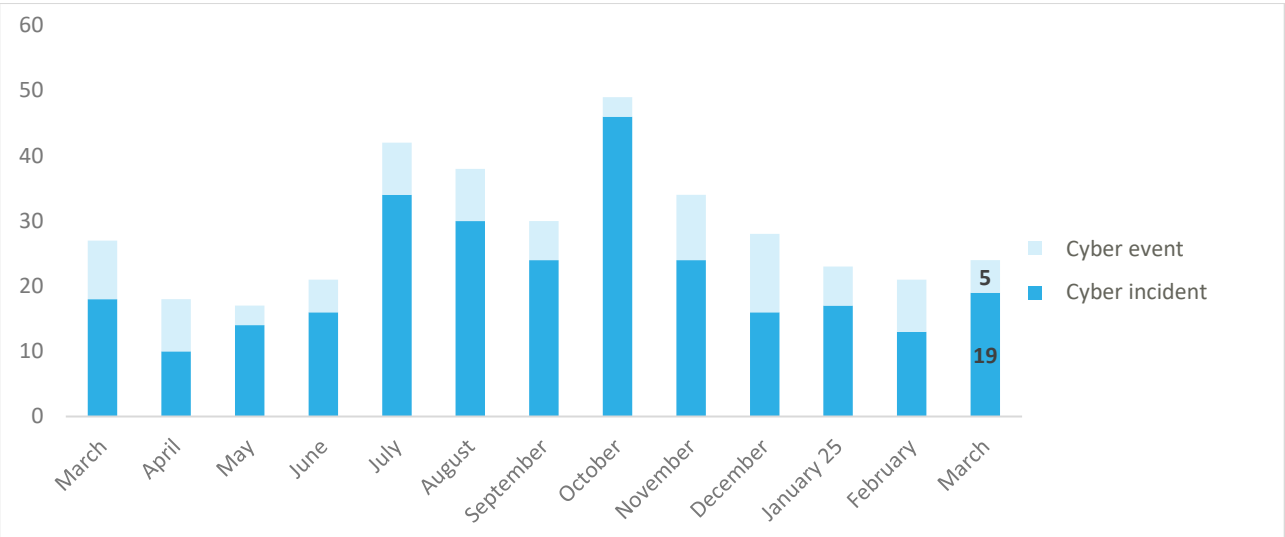
Severity of the handled cyber security incidents

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



Ratio of recorded cybersecurity incidents to cybersecurity events[1]

As part of its activities, NÚKIB receives, processes and evaluates reports related to cybersecurity. Based on the analysis, each report is classified as either a cybersecurity incident, a cybersecurity event or a non-relevant submission. The graph below illustrates the ratio between recorded cybersecurity incidents and cybersecurity events.



[1] A cyber security incident is a breach of information security in information systems, or a breach of the security and integrity of services or electronic communications networks, resulting from a cybersecurity event.
It is an event that may compromise the confidentiality, integrity, or availability of information systems or networks.
Both terms are defined in the Cybersecurity Act.

Classification of incidents reported to NÚKIB

The classification of cyber incident reported to NÚKIB follows the ENISA taxonomy: Reference Incident Classification Taxonomy — ENISA (europa.eu). The graphs below present the monthly distribution of incident categories over the past year. The numerical percentages indicate the proportion of each category relative to the total number of incidents reported in that particular month.

2024 **2025**

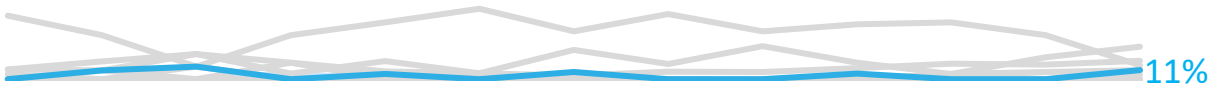
Availability – e.g. availability disruptions caused by a DoS/DDos attacks or acts of sabotage

Information content security – e.g. unauthorised access to data or unauthorised modification of information

Intrusion – e.g. compromising an application or user account

Malicious Code – e.g. virus, worm, trojan, dialer, spyware

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



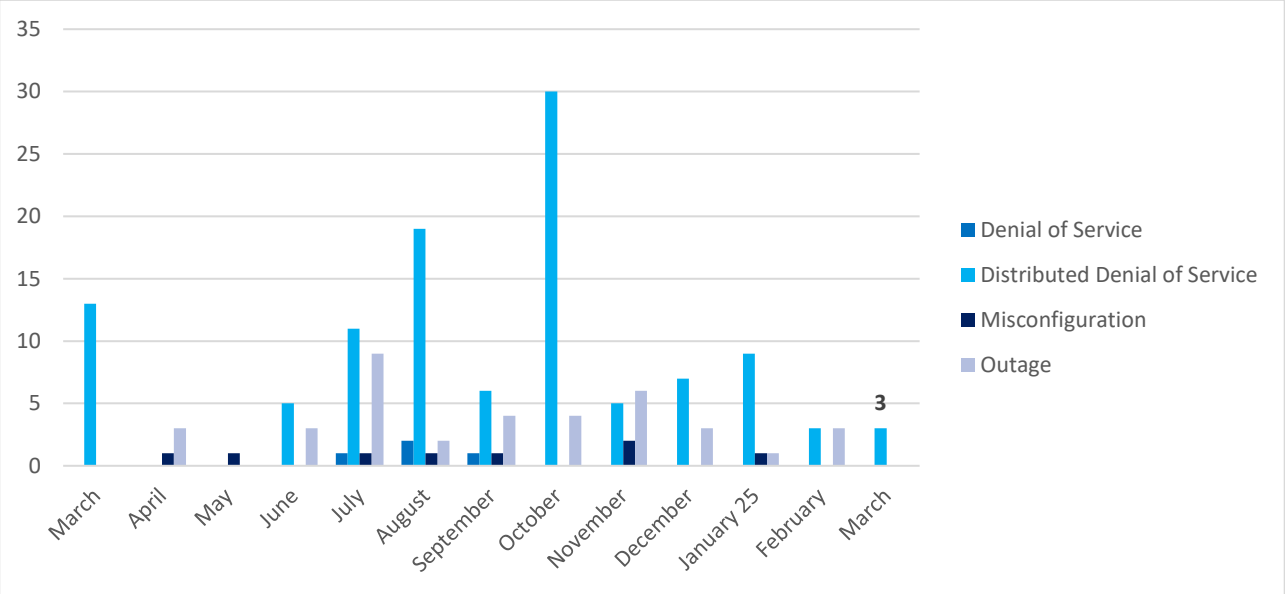
Other

Number of recorded incidents in selected categories

The categories presented below have been selected due to their long-term frequency (Availability) or severity (Information Security).

Availability

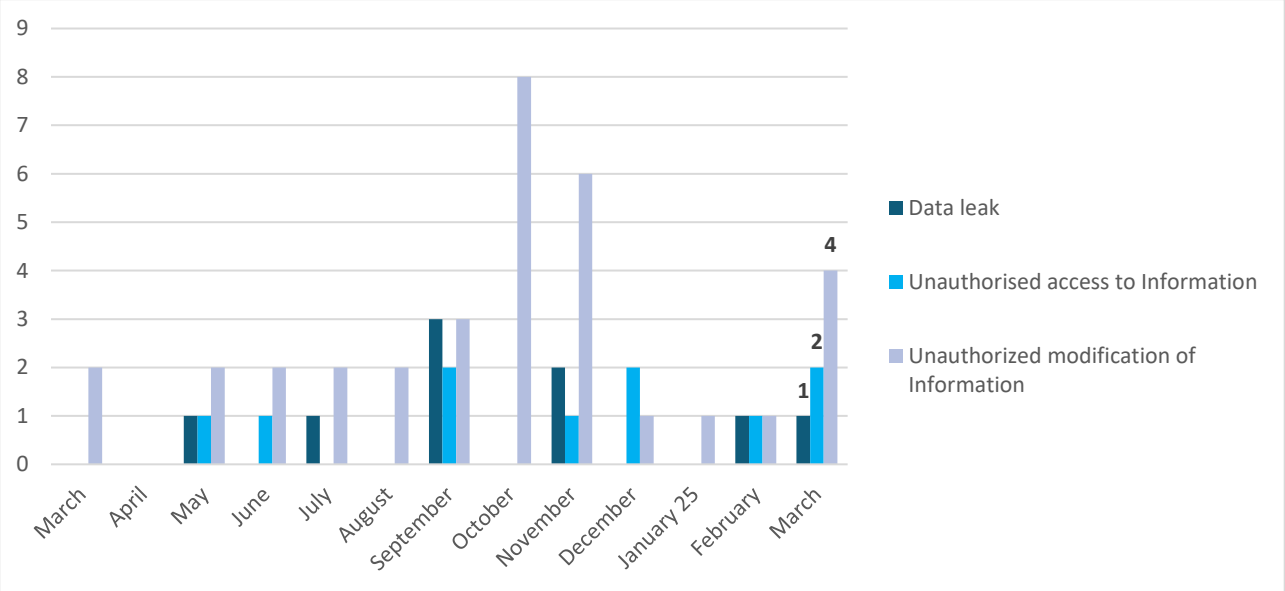
The Availability category is primarily includes incidents informing DDoS and DoS attacks. It also encompasses outages resulting from technical failures or misconfiguration or deliberate tampering.



Information Content Security

The Information Security category primarily consists of ransomware attacks, which are typically classified under the subcategory Unauthorized modification of information/data. It

also includes subcategories such as Unauthorized access to data and systems or Data leak.



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	15–35 %
Highly unlikely	0–10 %

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.