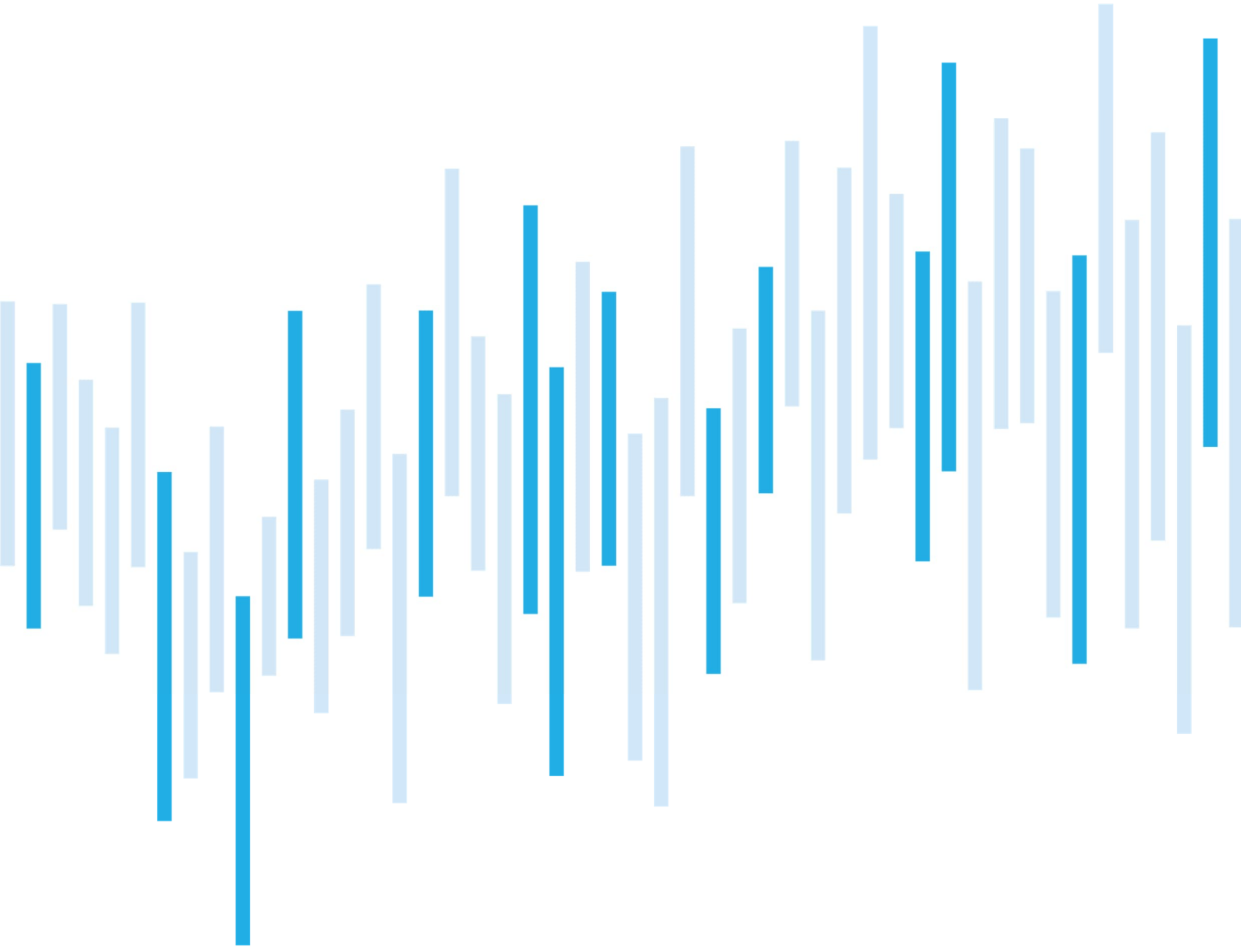
CYBER SECURITY INCIDENTS FROM THE NÚKIB'S PERSPECTIVE

JANUARY 2024



National Cyber and Information Security Agency

Summary of the month

In January 2024, there was a slight increase in incidents compared to December 2023. Despite this, NÚKIB recorded a below-average number of incidents for the third month in a row. In terms of the severity of recorded incidents, January copied the values of the previous two months. For the third month in a row, NÚKIB did not record any important or very important incidents.

Availability-related incidents were by far the largest category in 2023, and this trend also continued in January 2024. Further, NÚKIB dealt with incidents from the Information Content Security, Intrusion and Fraud categories.

Ivanti warned of several vulnerabilities related to Connect Secure (ICS) and Policy Secure (IPS) products during January. Due to active exploitation by state-sponsored and other actors, NÚKIB recommends immediate updates for the available versions of the vulnerable products or at least application of mitigation measures for versions where a patch is not yet available.

Table of content

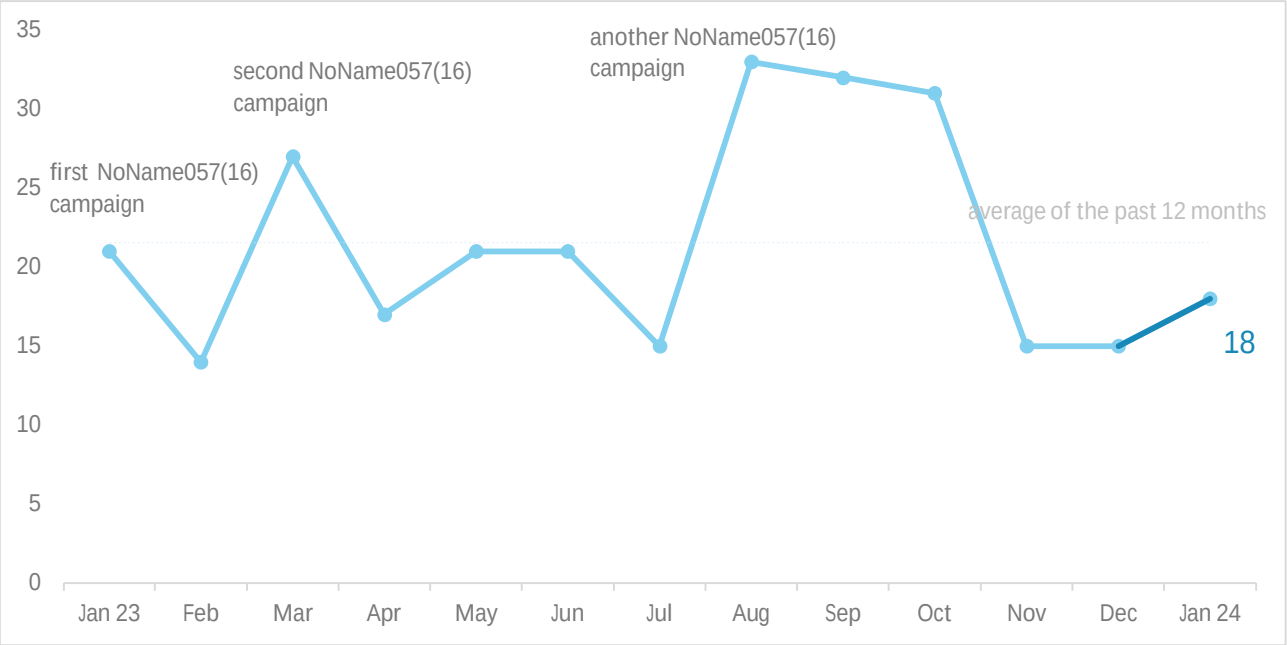
The following report summarises the events of the month. The data, information and conclusions contained herein are primarily based on cyber incidents reported to NÚKIB. If the report contains information from open sources in some sections, the origin of this information is always stated.

Some of the data in this report may differ from previous months' reports. At the turn of the year, NÚKIB made changes within the incident register system that have slightly altered the existing statistics on recorded incidents.

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

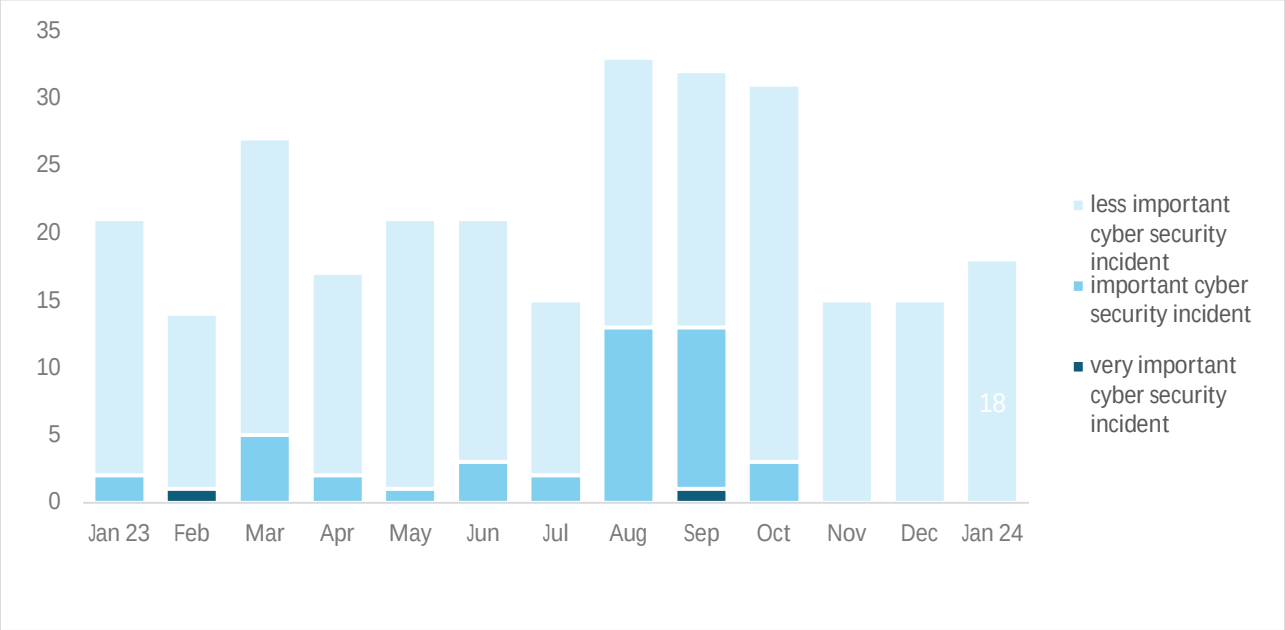
Number of cyber security incidents reported to NÚKIB[1]

In January 2024, there was a slight increase in incidents compared to December 2023. Despite this, NÚKIB recorded a below-average number of them.



Severity of the handled cyber security incidents[2]

In terms of the severity of recorded incidents, January was similar to the values of the previous two months. For the third month in a row, NÚKIB did not record any important or very important incidents.



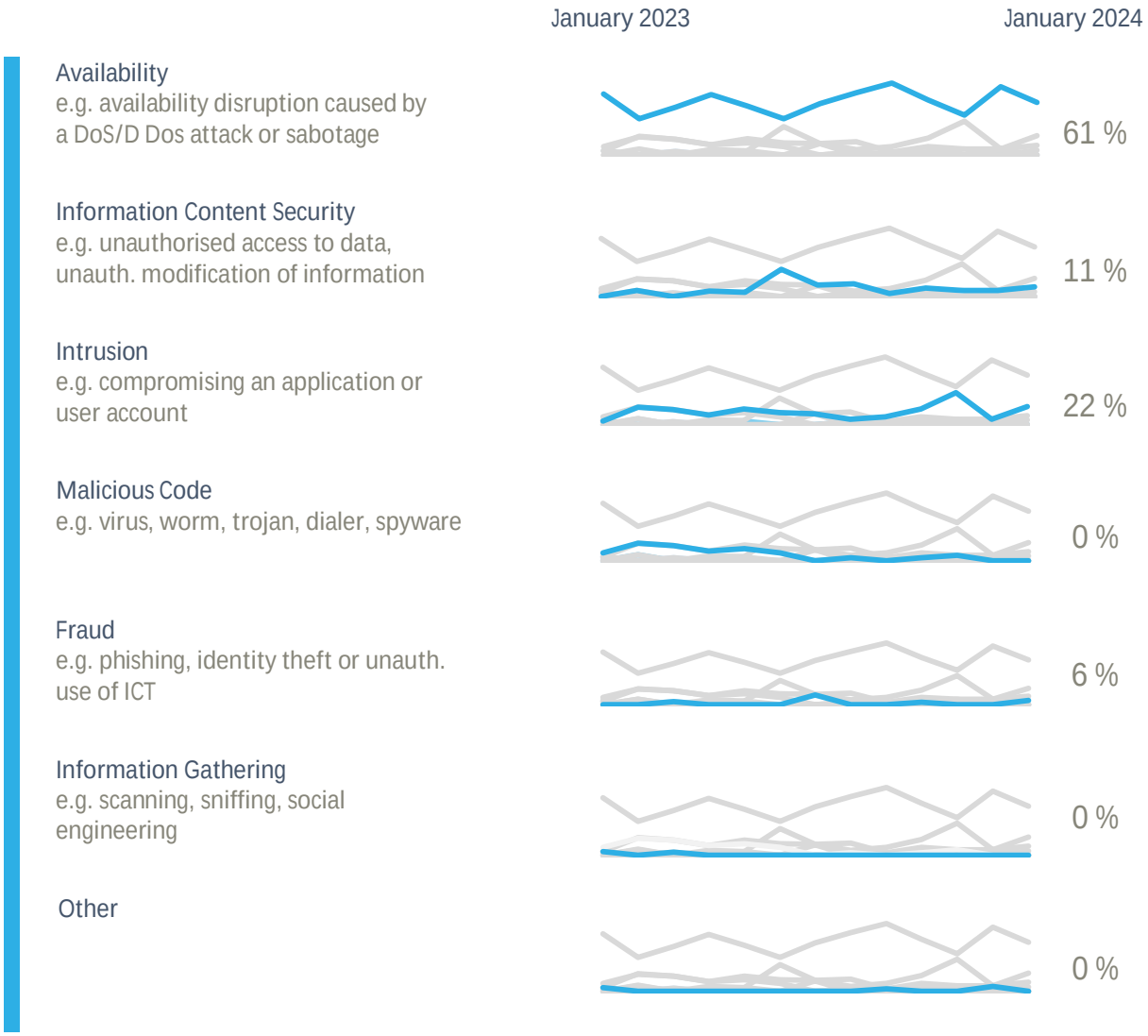
[1] NÚKIB registered 14 incidents in total with liable entities according to Cyber Security Act. The remaining 4 incidents involved unregulated entities.
[2] NÚKIB determines the severity of cyber incidents based on Decree No. 82/2018 Coll. and its internal methodology.

Classification of the incidents reported to NÚKIB [3]

Availability-related incidents were by far the largest category in 2023. This trend also continued in January 2024, although there was a proportionate decrease compared to the previous month (see charts below). Within the Availability category NÚKIB recorded both DDoS attacks and several technical failures.

In January NÚKIB registered incidents in three other categories.

- Four cases of Intrusion category were registered in January with only one case related to vulnerabilities in Ivanti products (see the Focus on a Threat chapter).
- Within the Information Content Security category, NÚKIB recorded one ransomware attack and one specific case in which attackers were to steal and subsequently offer data of an entity through compromising its suppliers.
- One registered fraud case involved a phishing email with a malicious link targeting higher dozens of employees of a regulated entity.



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

January trends in cyber security from the NÚKIB's perspective [4]

Phishing, spear-phishing and social engineering

In January, NÚKIB registered several phishing cases in which attackers managed to compromise targeted accounts or at least obtain the login credentials of victims.

Malware

Like in the previous months, also in January continuous malware analysis activities were conducted, focusing on selected incidents.

Vulnerabilities

At the beginning of January, NÚKIB warned of a Terrapin attack targeting the SSH protocol and exploiting the CVE-2023-48795 vulnerability. Most SSH client developers have already released a secure version, to which we recommend updating both the server and client too.

The vulnerabilities in Ivanti products, which are covered in the Focus on the Threat chapter, have become widely exploited in January.

Ransom ware

In January, as in December, only one ransomware-related incident was recorded, and that was with an unregulated entity. NÚKIB has not yet been able to verify what type of ransomware was involved.

Attacks on availability

NÚKIB recorded higher units of DDoS attacks during January. Pro-Russian hacktivist groups were behind some of the attacks, but the originator of most of them was not known.

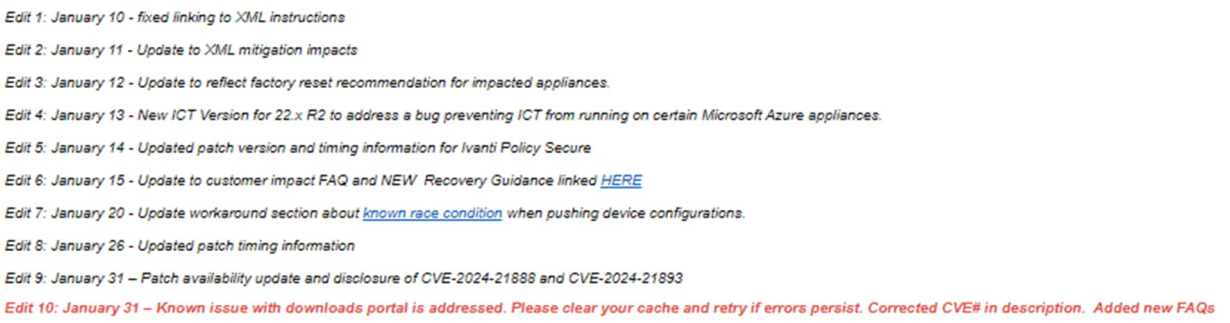
[4] The development illustrated by the arrow is evaluated in relation to the previous month.

Focus on a threat: Exploitation of vulnerabilities in Ivanti VPN products

On January 10, 2024, Ivanti warned of two zero-day vulnerabilities related to its Connect Secure (ICS) and Policy Secure (IPS) products. By combining the two vulnerabilities, an unauthenticated attacker can execute commands on all supported versions of ICS VPN and IPS network access control solutions. Vulnerabilities CVE-2023-46805 and CVE-2024-21887 should have been actively exploited against more than a dozen Ivanti customers at the time of the announcement. According to Volexity, so far unknown Chinese actor was to be behind this activity.

Shortly after the publication, massive exploitation of these vulnerabilities was reported worldwide. As early as January 15, Volexity suspected at least 1,700 compromised devices. US Cybersecurity and Infrastructure Security Agency (CISA) later warned of widespread exploitation of the vulnerabilities by a number of actors. In addition, during the investigation, the company discovered two additional vulnerabilities, CVE-2024-21888 and CVE-2024-21893, the latter of which had already been exploited against some customers

Fig. 1: Development of Ivanti's reaction to disclosed vulnerabilities in January



Source: forums.ivanti.com

The security patch for all of the vulnerabilities mentioned was delayed by Ivanti until January 31 and was released only for selected versions. Further patches are expected to be released gradually in the following weeks. At present, at least a vulnerability mitigation guide is available for these versions.

Due to active exploitation by state-sponsored or other actors, NÚKIB recommends immediate patch application for the available versions of the vulnerable products or at least to apply mitigation measures for versions where a patch is not yet available.

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	25–50 %
Unlikely	15–20 %
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://www.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	Limited disclosure, recipients can only spread this on a need-to-know basis within their organization. Note that 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.