CYBER SECURITY INCIDENTS FROM NÚKIB'S PERSPECTIVE

MAY 2025

National Cyber
and Information
Security Agency
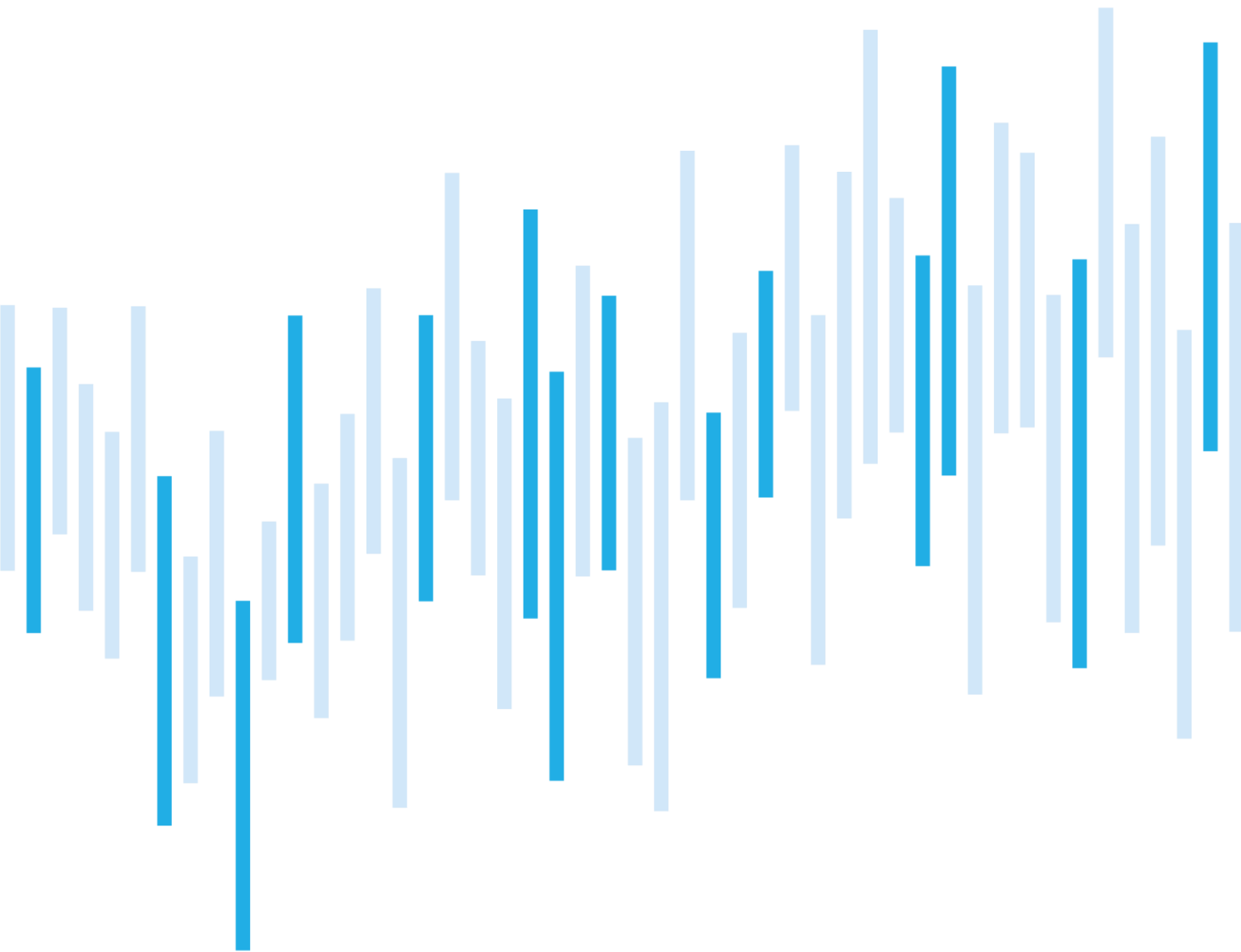
Summary of the Month

During May, NÚKIB recorded 11 cyber security incidents – the lowest number in the past twelve months. The most common category in May was Availability (4 incidents), with half of the incidents involving outages. The Information Security category (2 incidents) consisted exclusively of ransomware attacks targeting a secondary school and a private company. The Intrusion category (2 incidents) involved compromises of user accounts or servers. The Fraud, Abusive Content and Other categories each accounted for one incident, involving spam sent from a legitimate user's mailbox, fraudulent websites and brief website outages.

In terms of severity, all incidents in May were assessed as less significant. The number of cyber events in May was also low, with only 4 reported. These included examples such as fraudulent WhatsApp messages and phishing emails.

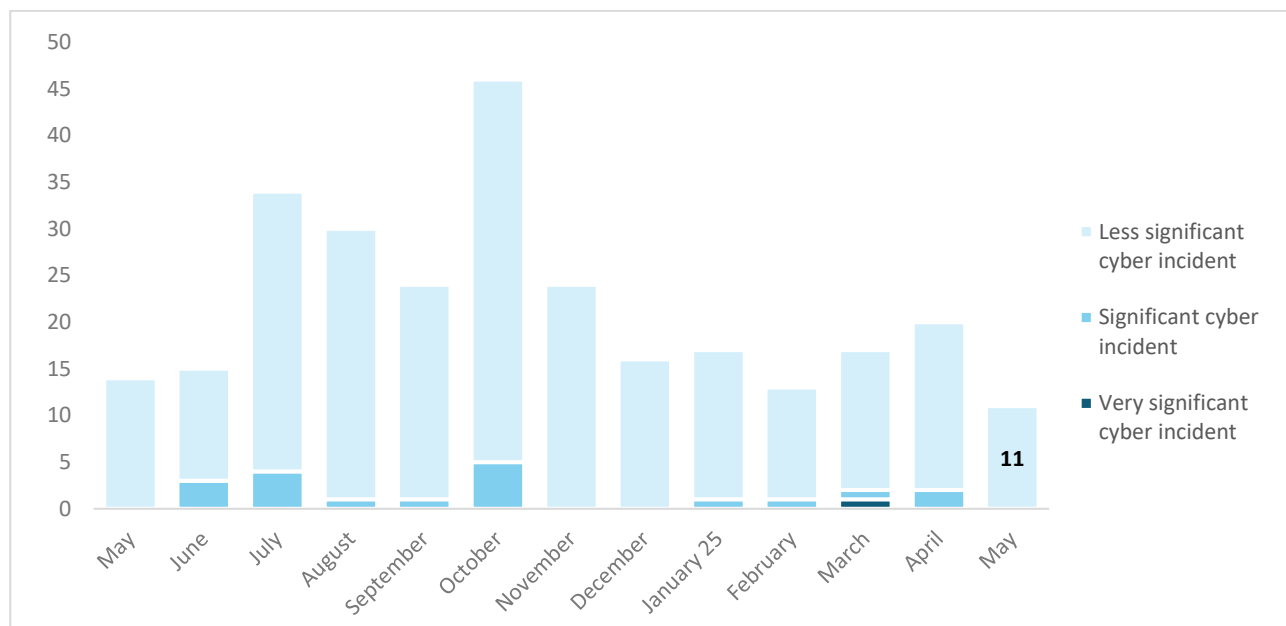## Number of cyber security incidents reported to NÚKIB
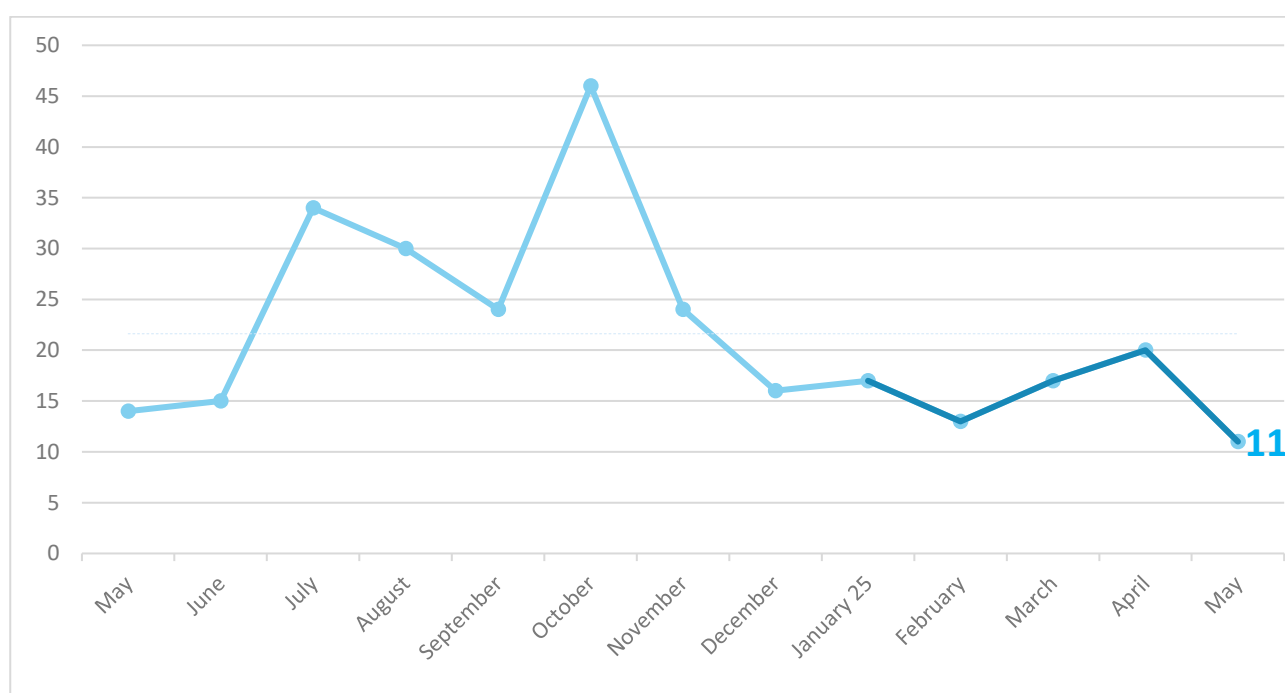
Severity of the Handled Cyber Security Incidents

The severity of cyber incidents is assessed by NÚKIB in accordance with 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 a cybersecurity incident, a cybersecurity event, or a non-relevant submission. The graph below illustrates the ratio between recorded cybersecurity incidents and cybersecurity events.
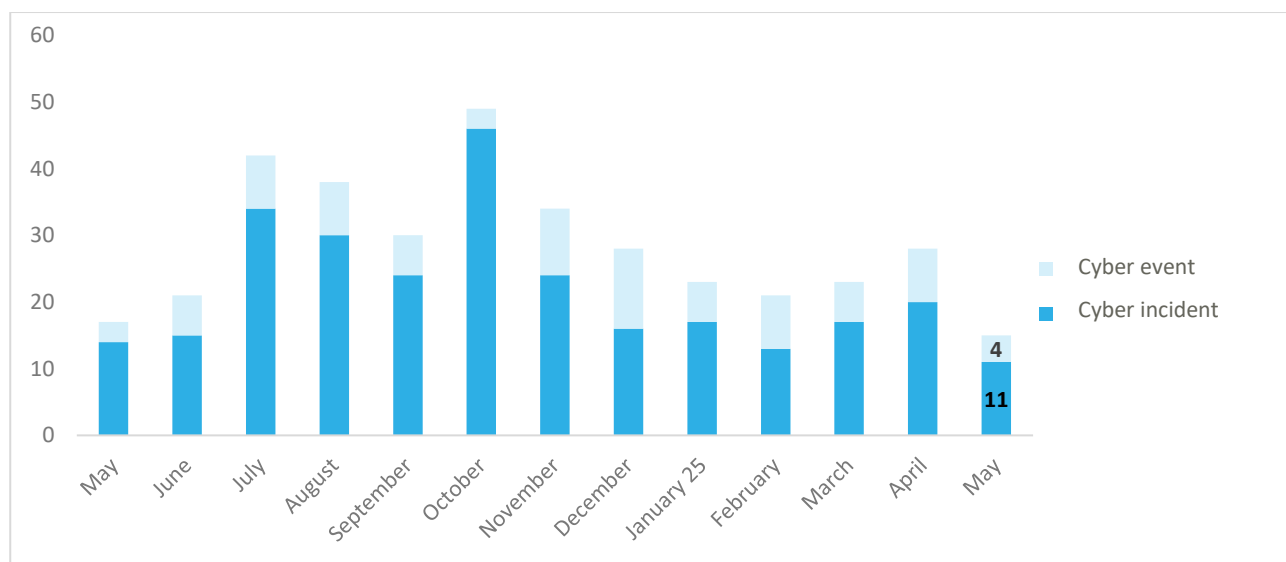
[1] A cyber security incident is a breach of information security in information systems, or a breach of the security and integrity of services or electronic communications networks, resulting from a cybersecurity event.
It is an event that may compromise the confidentiality, integrity, or availability 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, as outlined in the Reference Incident Classification Taxonomy — ENISA (europa.eu). The graphs below show the monthly distribution of incident categories over the past year. The numerical percentages represent the share of each category relative to the total number of incidents reported in the respective month.

2024   **2025**

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

36%

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

18%

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

18%

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

0%

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

9%

**Abusive Content**

9%

Other

9%

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 primarily includes incidents related to DDoS and DoS attacks. It also covers outages caused by technical failures, misconfiguration or deliberate tampering.
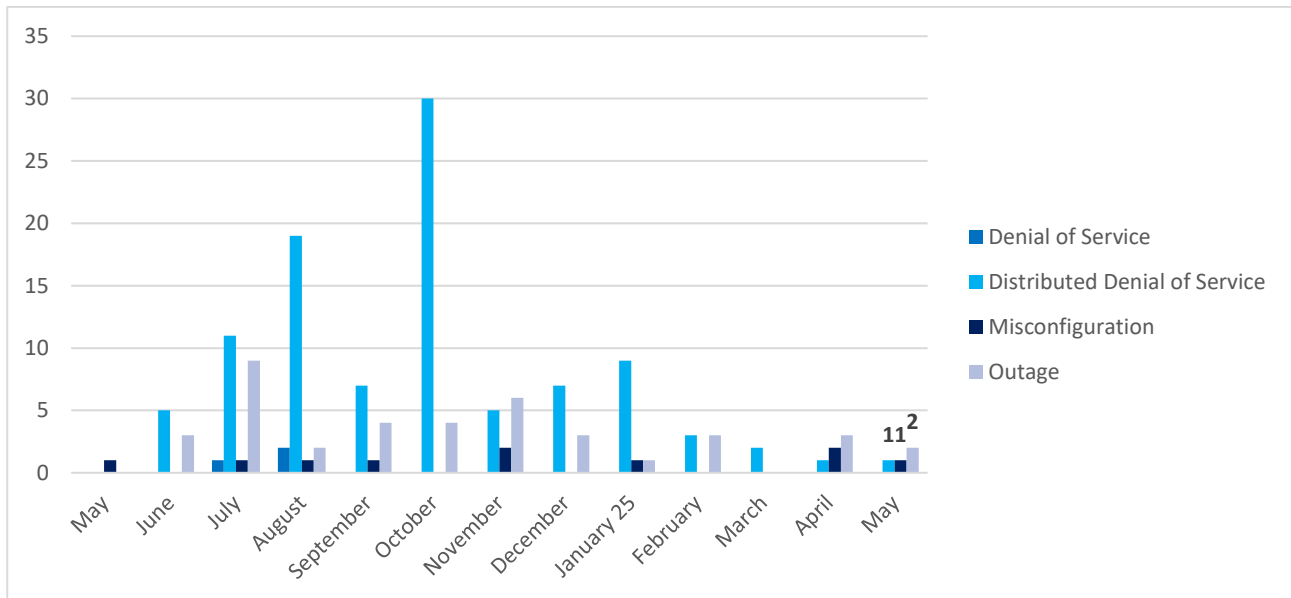
Information Content Security

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

also includes other subcategories such as Unauthorized access to data and systems and Data leak.
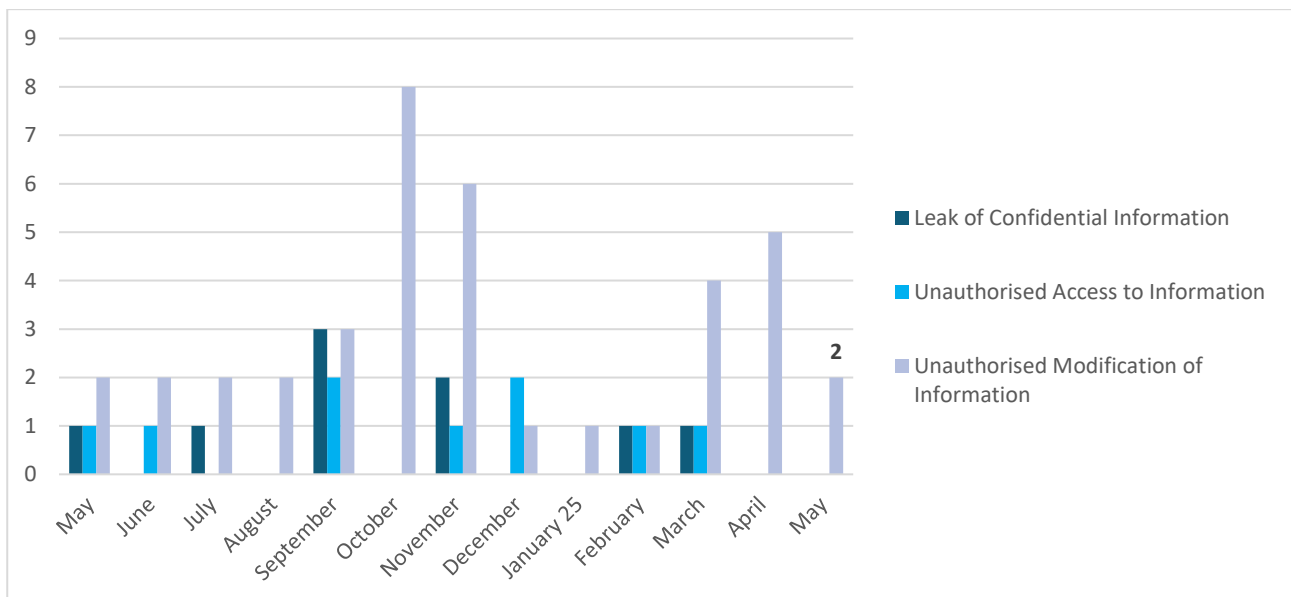
Probability terms used

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. This designation is used when disclosure could pose significant risks to the privacy, reputation, or operations of the organizations involved, and when effective action cannot be taken without such risks. Recipients are therefore strictly prohibited from sharing TLP:RED information with others. For example, in a meeting setting, TLP:RED information may only be shared with those present in the room at the time of disclosure.
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 its clients. Sources may use TLP:AMBER when the information requires support to be effectively acted upon, but poses 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 the information 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 may share this information freely, there are no restrictions on its 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.