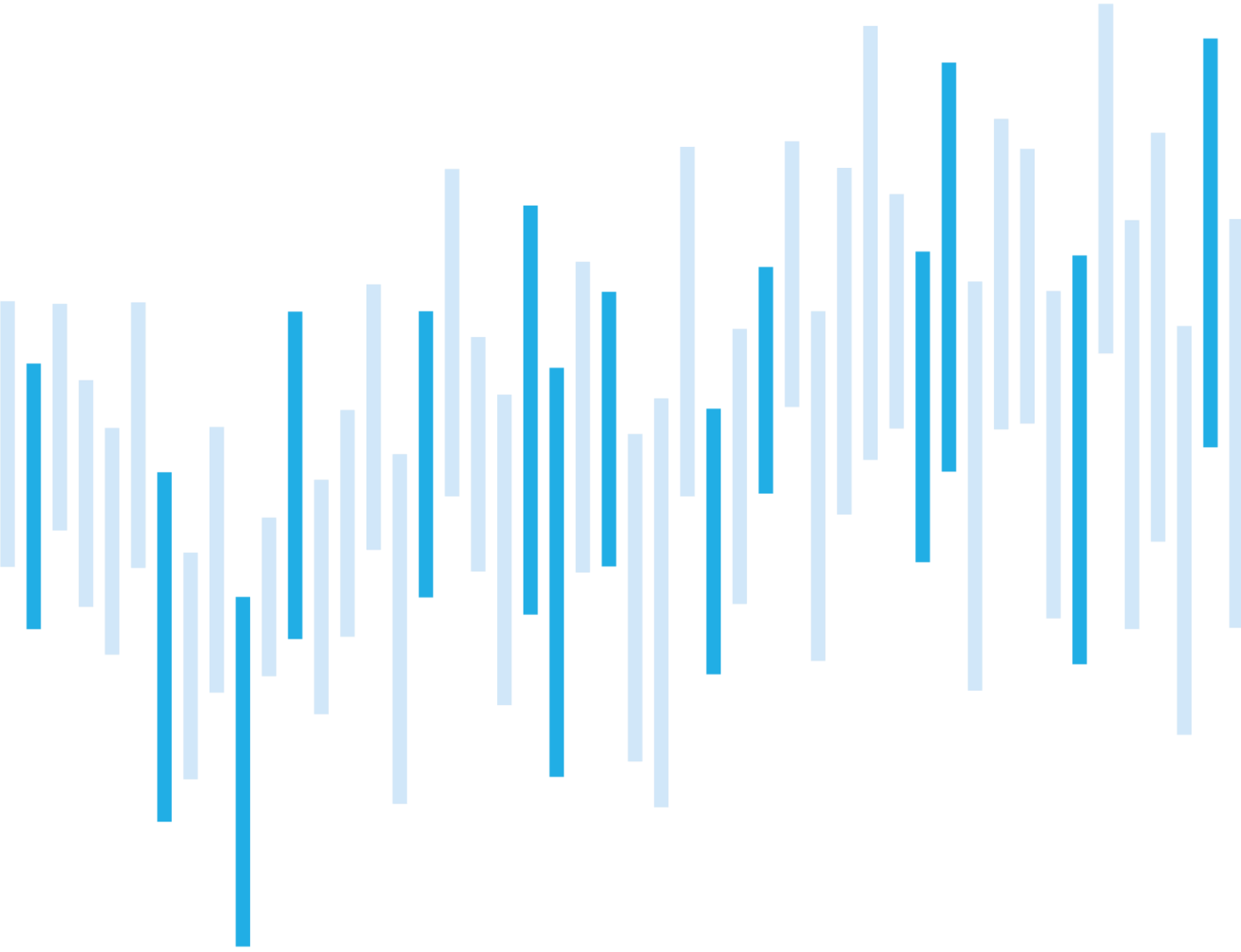
CYBER INCIDENTS FROM THE NÚKIB'S PERSPECTIVE

JANUARY 2022



Národní úřad
pro kybernetickou
a informační bezpečnost

Summary of the month

January was an average month in terms of number of incidents. Since the publishing of the Log4Shell vulnerability, it was the first time NÚKIB registered an incident in which its abuse preceded a ransomware attack. Having discovered this vulnerability in a virtualisation management programme of a private company, the attackers managed to penetrate the company's system and launch the NightSky ransomware. It is a new ransomware, which first appeared in the second half of December, not long after the Log4Shell vulnerability had been published.

The public also informed NÚKIB about vulnerabilities of systems belonging to two regulated entities. We thank for all the notices. Weaknesses and vulnerabilities in systems exposed to the Internet belong to the most frequent attack vectors, which is one of the reasons why we are currently dealing with the both cases.

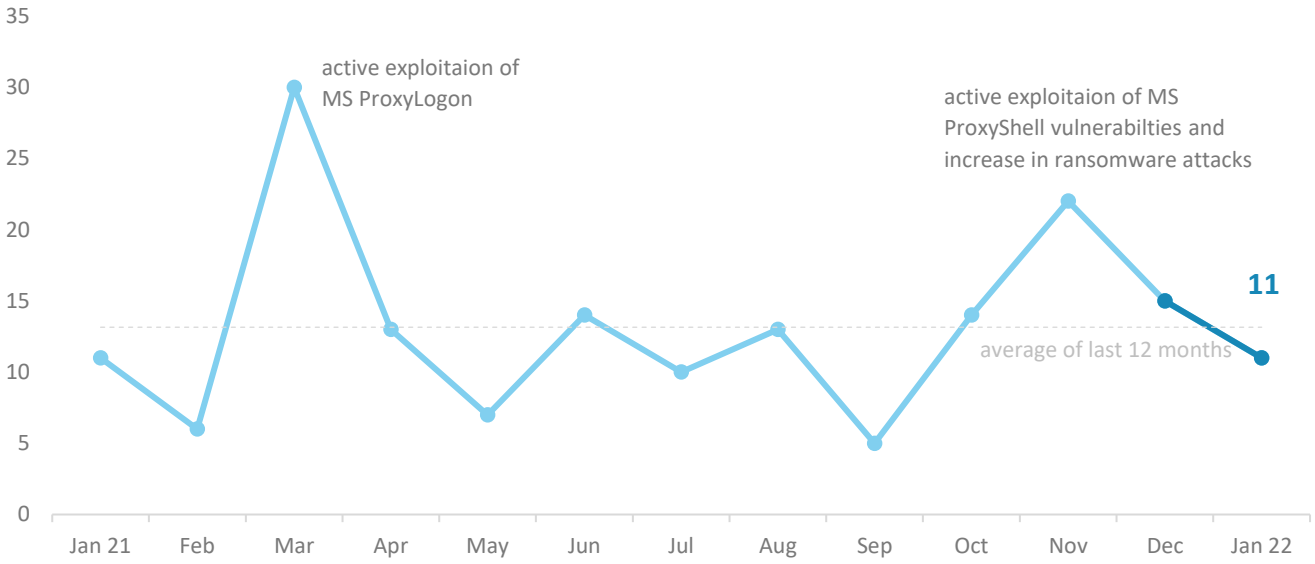
Table of contents

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

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

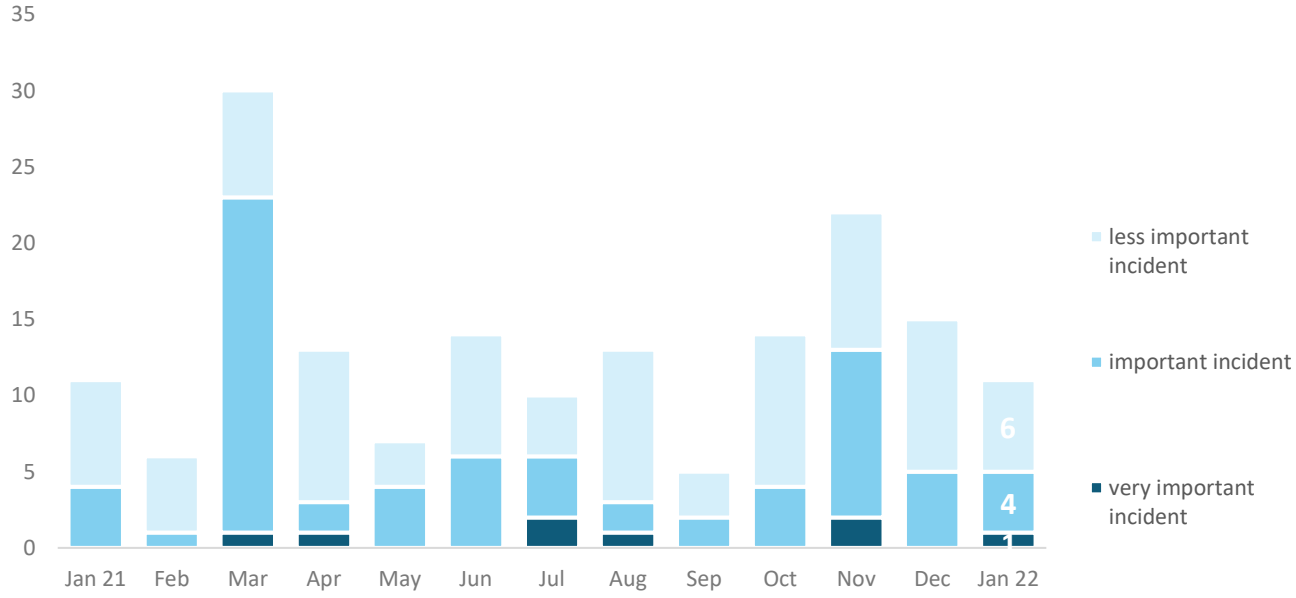
Number of cyber security incidents reported to NÚKIB

Regarding the number of incidents, January was slightly below the last year's average.[1]



Severity of the handled cyber incidents[2]

One of January's incidents is registered by NÚKIB as very important. It was caused by a faulty component in infrastructure of the affected organisation, but the impact was so severe that the incident was categorised within the highest severity possible. It involved an outage of a critical infrastructure element and had a nation-wide impact.

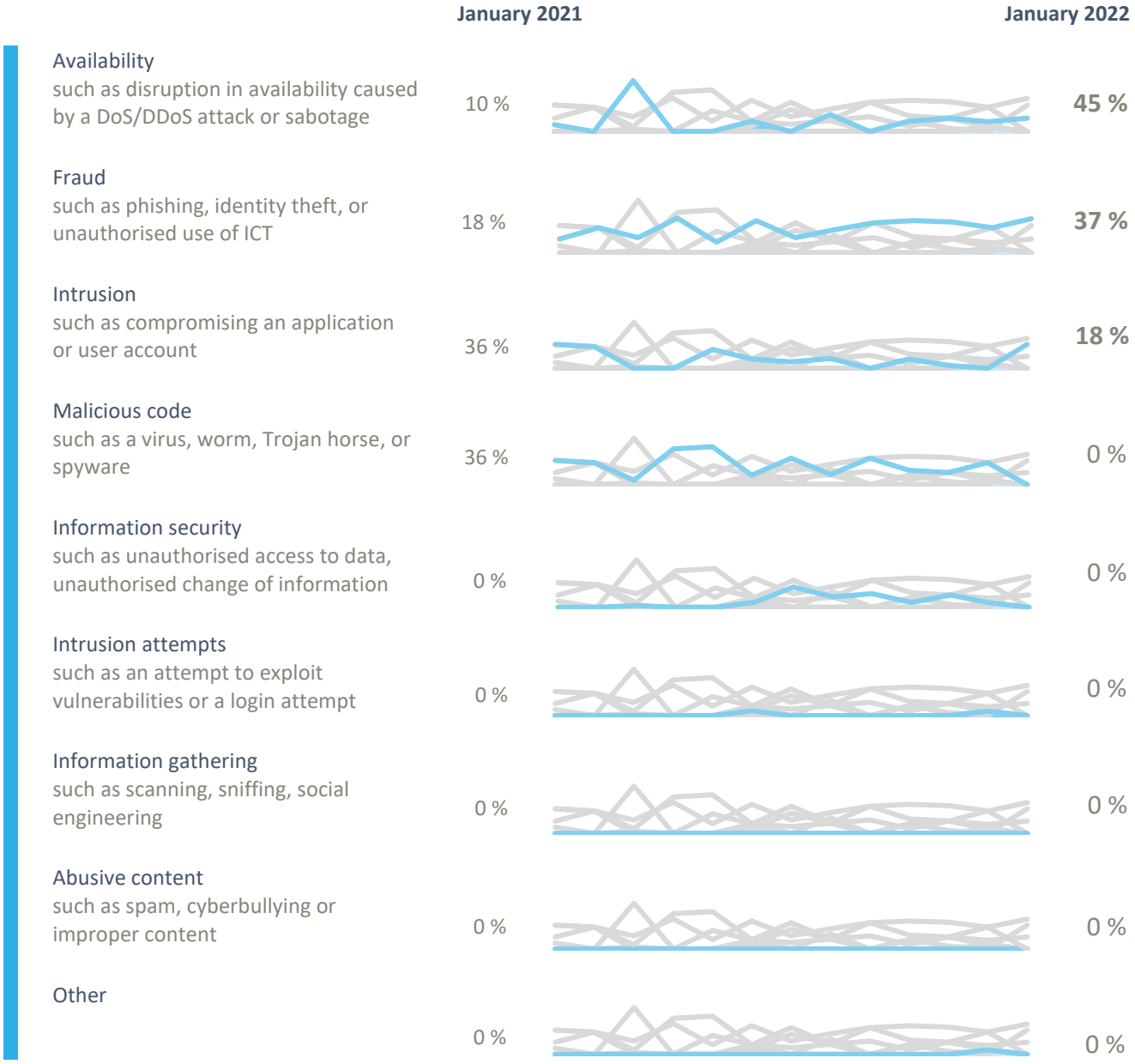


[1] Seven incidents were reported to NÚKIB by regulated persons according to the Cyber Security Act. The remaining four incidents were reported to NÚKIB by entities that do not fall under this law.
[2] The severity of cyber incidents is defined in Decree No. 82/2018 Coll. and in NÚKIB's internal methodology.

Classification of the incidents reported to NÚKIB[3]

January's incidents were divided into three categories:

- Five incidents resulted in the unavailability of a service. In two of the cases, the organisation's functioning was affected by ransomware, which encrypted not only data but also the backups of its victim. In the remaining three cases, the unavailability was caused by a technical error;
- The second most frequent category with four incidents was fraud, mainly caused by phishing campaigns in public administration. Beside the phishing, this category of incidents also included financial fraud in a public company. The attackers used an unknown method to get into the e-mail box of a user responsible for sending invoices to business partners and changed the payment details in the invoices. Then they sent the forged account numbers to at least two foreign companies and thus got thousands of euros from them;
- NÚKIB classified the last two incidents as intrusion because attackers got into their victims' networks by exploiting vulnerabilities, including the Log4Shell vulnerability.



[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

At the beginning of the year, NÚKIB registered two phishing campaigns that affected Czech public institutions. In both cases, the attackers managed to compromise user accounts and send from them further phishing to various other organisation, including public institutions. In one of the campaigns, the attacker used the so-called thread hijacking when they continued in already existing communication of their victim and sent messages with harmful links in replies to those threads. The attacked organisation managed to solve the situation within 24 hours of the compromising; however, we do not know yet how many users from

Malware

Apart from the ransomware below, January's incidents did not include any other malicious code.

Vulnerabilities

Exploitation of the Log4Shell vulnerability continued in January. The vulnerability caused two of the incidents addressed by NÚKIB. In the first case, the attackers compromised a server for the administration of mobile devices located in a public administration institution but did not cause any further damage. In the second case, described in part "Ransomware", the attackers firstly exploited the vulnerability in VDI VMware Horizon and then installed ransomware in systems of a Czech private company and encrypted its files.

The public also informed NÚKIB about vulnerabilities of domains belonging to two regulated entities. NÚKIB is currently addressing both cases.

Ransomware

NÚKIB addressed two ransomware cases in January, which represents a decrease in their number compared to the preceding two months. The first was Jigsaw ransomware in a public organisation and the other NightSky ransomware in a private company.

The NightSky case is interesting as it was probably the first Czech case when attackers abused the Log4Shell vulnerability to get into their victim's network and then encrypted its systems. NightSky is a new ransomware that first appeared in the second half of December 2021, i.e. not long after the vulnerability was published. According to Microsoft, it is used in a campaign by a Chinese group, which they named DEV-0401. However, we cannot rule out the ransomware used another actor.

Attacks on availability

Although nearly half of January's incidents ended up with the unavailability of a service, none of them was caused by a DoS or DDoS attack.

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

Technique of the month: User Execution

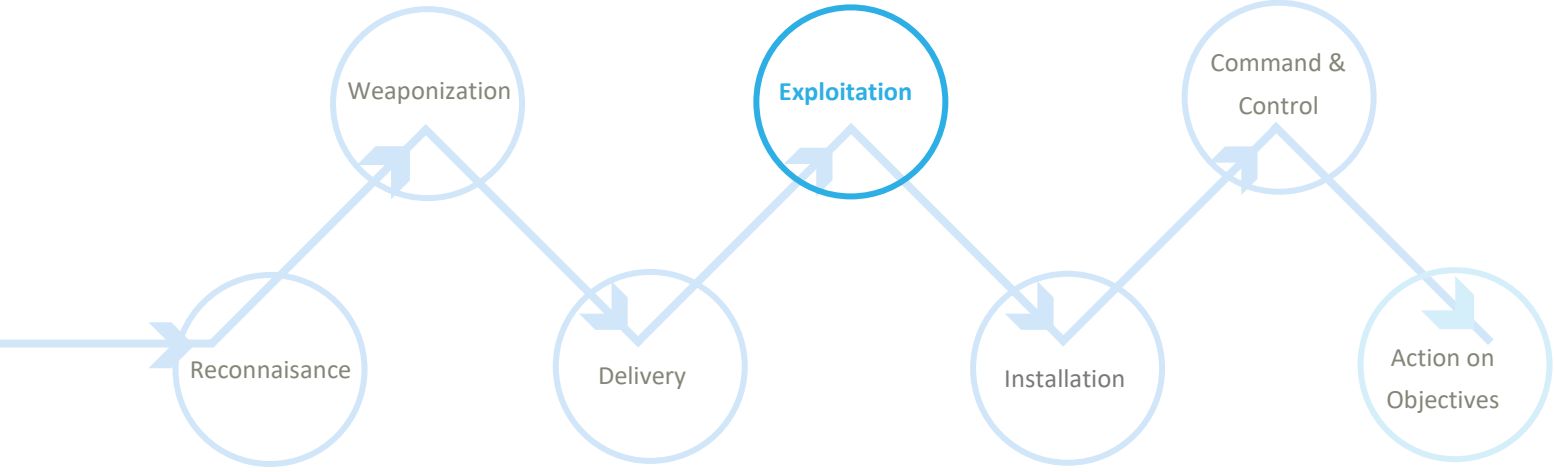
In January, the incidents most often included a technique that MITRE ATT&CK calls "Exploit Public-Facing Application"; it is mainly connected with exploiting vulnerabilities in infrastructures exposed to the Internet. We already described this technique in the August report. Therefore, we are focusing on the "User Execution" technique, which was the second most widely used technique in January, and which is connected to the incidents associated with phishing.

User Execution is a technique during which attackers rely on a user help to them to compromise the system. They, therefore, often opt for social engineering and try to mislead users so that they unconsciously launch a malicious code or provide them with credentials. A typical example is phishing messages in which attackers try to make their victims open an infected e-mail or fill their data in forged login pages. The registered January incidents mainly included efforts to extract credentials from users.

MITRE ID: T1204

Mitigation: Mitigation of this technique is performed at two levels. At the technical level, a considerable amount of phishing relying on a forged identity of the sender can be filtered out, providing that the mail server supports and performs incoming mail checking in compliance with NÚKIB's safeguard measure. Other suitable counter-measures include attachment sandboxing, at least with potentially problematic file types (zip, exe, ps1, js), and warning in the case of archives requiring passwords. The most often method of delivering malware is still macros in Office documents. The easiest way is to disable Macros by group policies for those users who do not need it for their work. However, these technical steps per se are not sufficient. It is necessary to train users continuously, pointing out the risks associated with social engineering and the latest trends in phishing so that they can detect them themselves.

A representation of "User Execution" in a kill chain showing at which point attackers use the technique:



Focused on a sector: Public administration

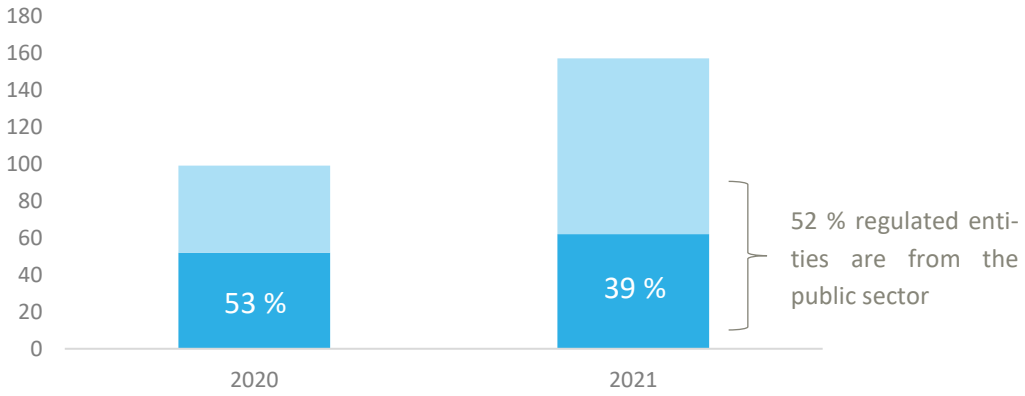
Almost two-thirds of January's incidents occurred in the public sector. They included successful phishing campaigns, ransomware, and also intrusion caused the Log4Shell vulnerability.

7 cyber incidents

64% representation in January's incidents

Attacks on the public sector are the most frequent among those registered by NÚKIB. The public sector has been the most affected sector over the last two years. In 2021, the share of cyber incidents rose to nearly 40 % of all addressed incidents. One of the main reasons for the high share of incidents in the public sector is that more than half of the regulated persons, i.e. organisations obliged to notify NÚKIB about incidents under the Cyber Security Act, are public administration institutions.

The share of incidents in the public sector of the total number of incidents



The public sector is generally a tempting target for attackers, both APT groups sponsored by foreign states and cyber-criminal groupings.

APT groups mainly perform more sophisticated attacks against ministries and other institutions of central public administration, which are a source of information of intelligence, military, political, and economic importance. Cyber espionage operations seeking to gain similar information are of a long-term character and require the attackers to have the advanced capability to avoid detection in the long run and exfiltrate data from the attacked system unnoticed. Mainly state actors or groups sponsored by them have such a level of know-how. Neither the Czech Republic is spared from such attacks; NÚKIB already handled several of them in the past.

The incidents registered by NÚKIB often include attacks on local authorities. In 2020, it mainly was ransomware (70% of incidents in the self-government sphere). In 2021, ransomware attacks on local authorities were less frequent (17%), while compromising through vulnerability dominated (58%). For attackers, local authorities are tempting targets because of the possibility of financial gain. Based on our experience, both large cities with the possibility of higher gain and smaller towns with often underfunded cyber security, where attackers do not expect strong security, are endangered.

Probability Terms Used

Probability terms and expression 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 %

Conditions for the Use of Information

The information provided shall be used in accordance with the Traffic Light Protocol methodology (available at the website www.nukib.cz). 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
TLP:RED	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.
TLP:GREEN	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction