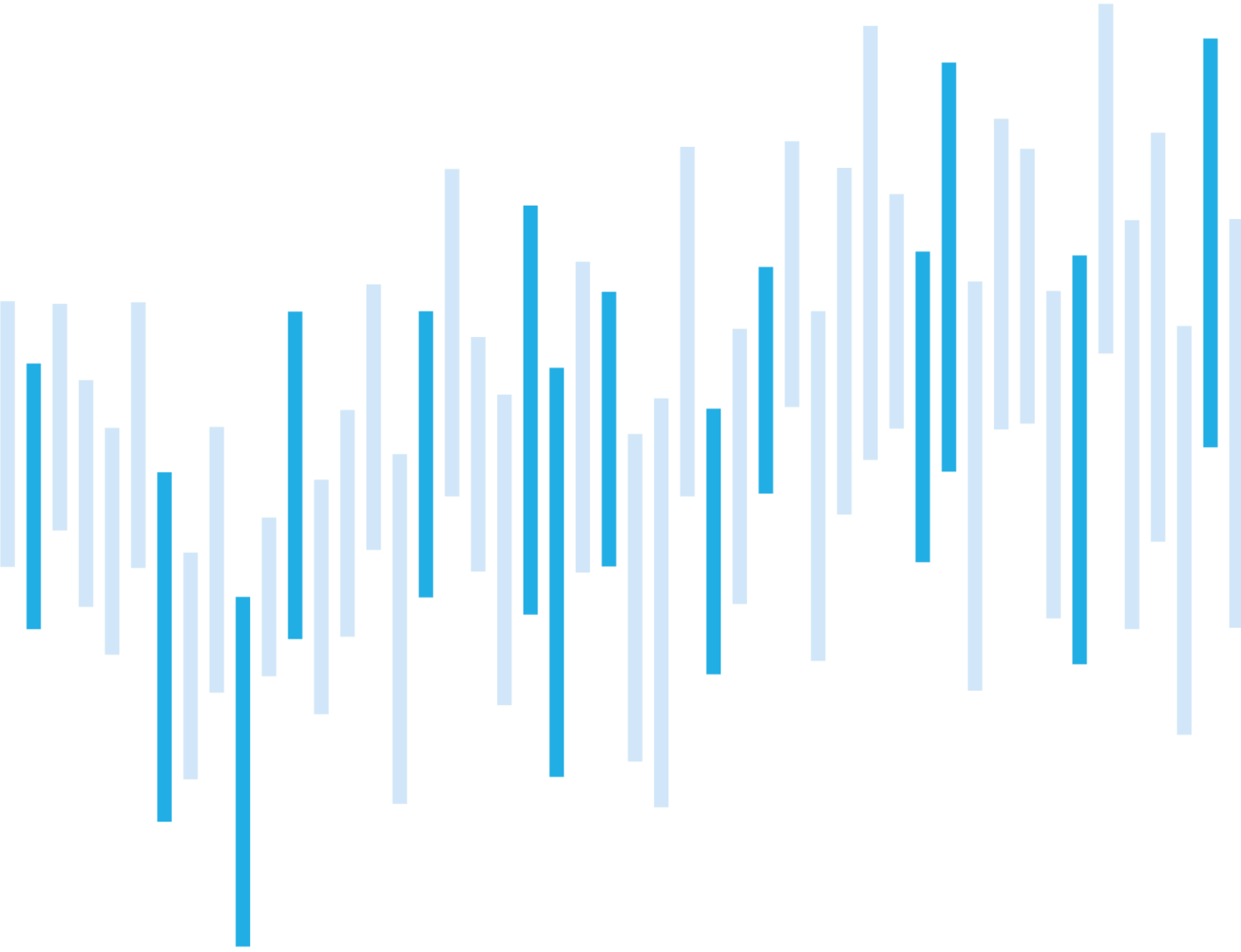
CYBER SECURITY INCIDENTS FROM THE NÚKIB'S PERSPECTIVE

MAY 2022



National
Cyber and Information
Security Agency

Summary of the month

After the preceding busy month, the number of cyber incidents dropped back to average in May. Nevertheless, the incidents were rather severe.

The incidents in May were marked with poor security on the side of suppliers, which the attackers exploited to gain access to their victims' networks. Therefore, this report focuses on the management of suppliers. Chapter Technique of the Month outlines how attackers can exploit suppliers' poor security and the last chapter describes the supplier management as a security measure.

The new critical vulnerability CVE-2022-30190, known as "Follina", needs to be highlighted among May events. Follina is associated with Microsoft Office suite and makes phishing attacks much easier. Attackers can launch malicious code via this vulnerability even without the victim enabling macros. Hacker groups worldwide have immediately started to exploit this vulnerability. NÚKIB did not register any exploit of this vulnerability among May incidents, but it cannot be ruled out that the situation will change in the following days. Since the vulnerability is relatively easy to exploit and no patch is available yet, it cannot be ruled out that a similar wave of cyber attacks will come, as in the case of the MS Exchange vulnerability exploitation in 2021.

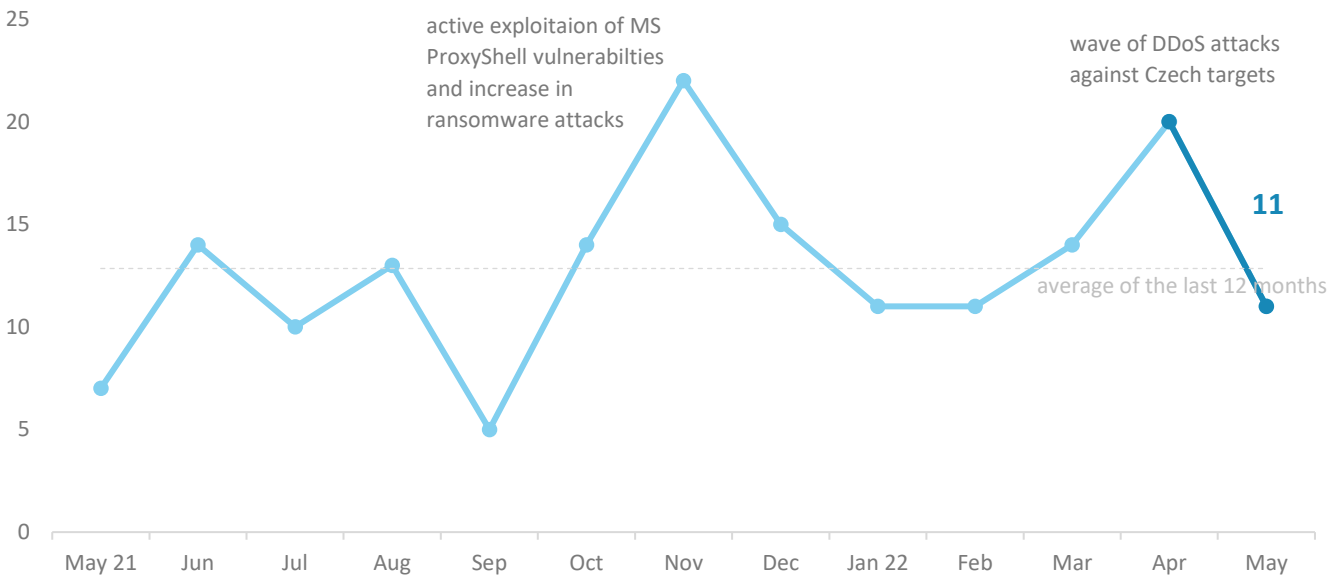
Table of contents

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 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.cz.

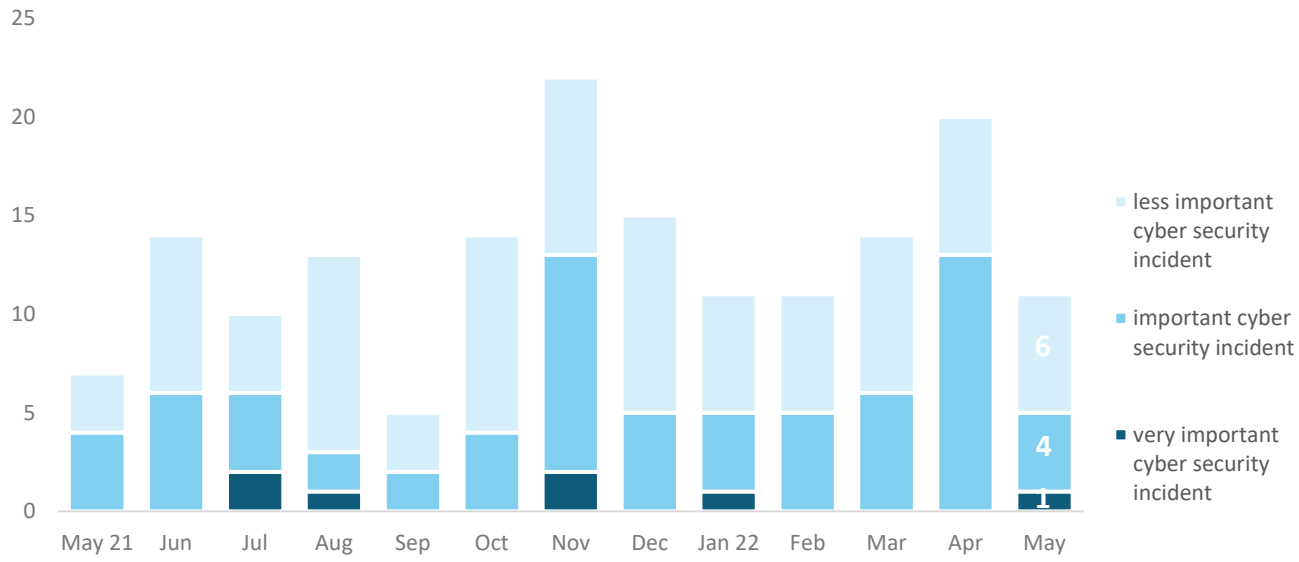
Number of cyber incidents reported to NÚKIB

After the busy April, the number of incidents returned to the average of the preceding twelve months.[1]



Severity of the handled cyber incidents [2]

A very significant incident occurred after three months. Attackers managed to compromise a network with critical systems, preventing the attacked organisation from performing its duties and causing widespread damage.

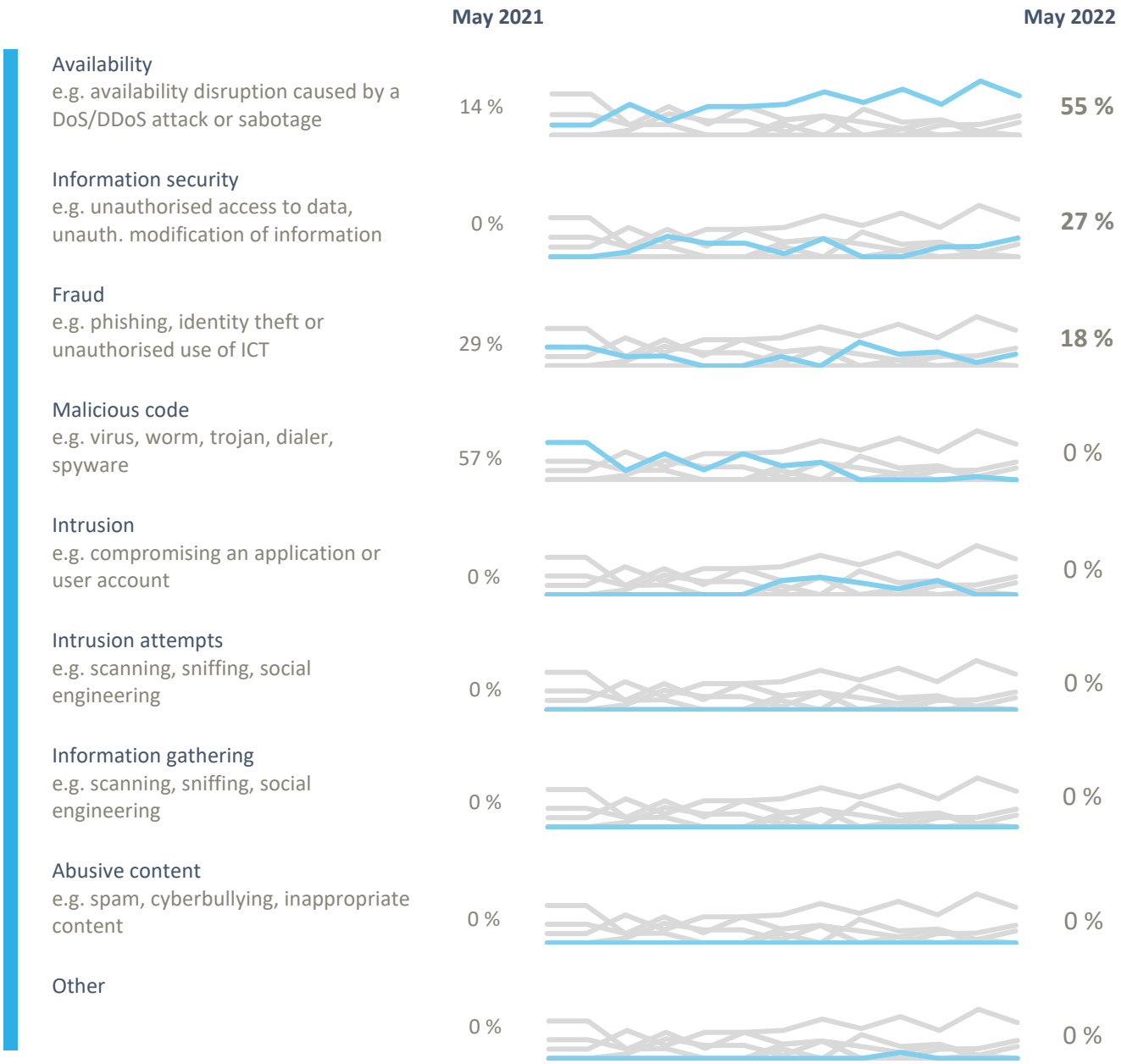


[1] Nine of the incidents were reported to NÚKIB by obligated persons according to the Cyber Security Act. The remaining two incidents were reported by entities that do not fall under this law.
[2] NÚKIB determines the severity of cyber incidents on the basis of Decree No. 82/2018 Coll. and its internal methodology.

Classification of the incidents reported to NÚKIB[3]

NÚKIB classified May's incidents within the following three categories:

- More than half of the cyber incidents resulted in the unavailability of services. But for one case, the cases of service unavailability were caused by technical failures. The only exception was a cyber incident caused by ransomware, which the attackers used to encrypt the victim's data and back-ups;
- The second most frequent category included incidents involving unauthorised access to information. This category also includes a ransomware attack, during which the attackers exfiltrated data of the attacked organisation before encrypting it;
- In two cases, NÚKIB classified the incidents as fraud. Both the incidents involved phishing. The first extensive phishing campaign targeted clients of a commercial bank. The attackers tried to gain credentials to their Internet banking and then transfer money from it. The second phishing was detected at a moment when phishing e-mails were sent from the domain of the attacked educational institution to other addresses.



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

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

Phishing, spear-phishing, and social engineering

Phishing attacks regularly occur in the incidents reported to NÚKIB (see Fraud category in the graph on the previous page). The most serious of the attacks in May was an extensive and targeted campaign against clients of a Czech commercial bank. Using fraudulent SMS and e-mails, the attackers tried to gain access to their Internet banking and consequently transfer money from their accounts. The attackers tried to intrigue the bank's clients into opening a malicious link by stating that their bank account had been blocked and that they had to log in again to unblock it.

Malware

Based on data from May's incidents, NÚKIB did not analyse any malware apart from the ransomwares mentioned below.

Vulnerabilities

A new critical vulnerability CVE-2022-30190, also known as "Follina", of the Microsoft Office suite was discovered at the end of May. It allows the attackers to launch a malicious code without a victim enabling macros. Phishing attacks are hence much easier. Hacker groups, including APT groups supported by governments of third countries, immediately started to exploit it. Therefore, NÚKIB warned about the vulnerability on its web pages and recommended how to mitigate the vulnerability until a patch is available.

Ransomware

Since the beginning of the year, ransomware attacks have continuously represented approximately one-fifth of the incidents reported to NÚKIB. In this respect, May was no exception. Two of the incidents were caused by ransomwares-as-a-service, which attackers have been deploying across cyberspace since summer 2021.

Attacks on availability

While April was characterised by waves of DDoS attacks against Czech targets, May was a calm month in this respect. None of the incidents handled by NÚKIB was caused by a DDoS attack.

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

Technique of the month: Trusted Relationship

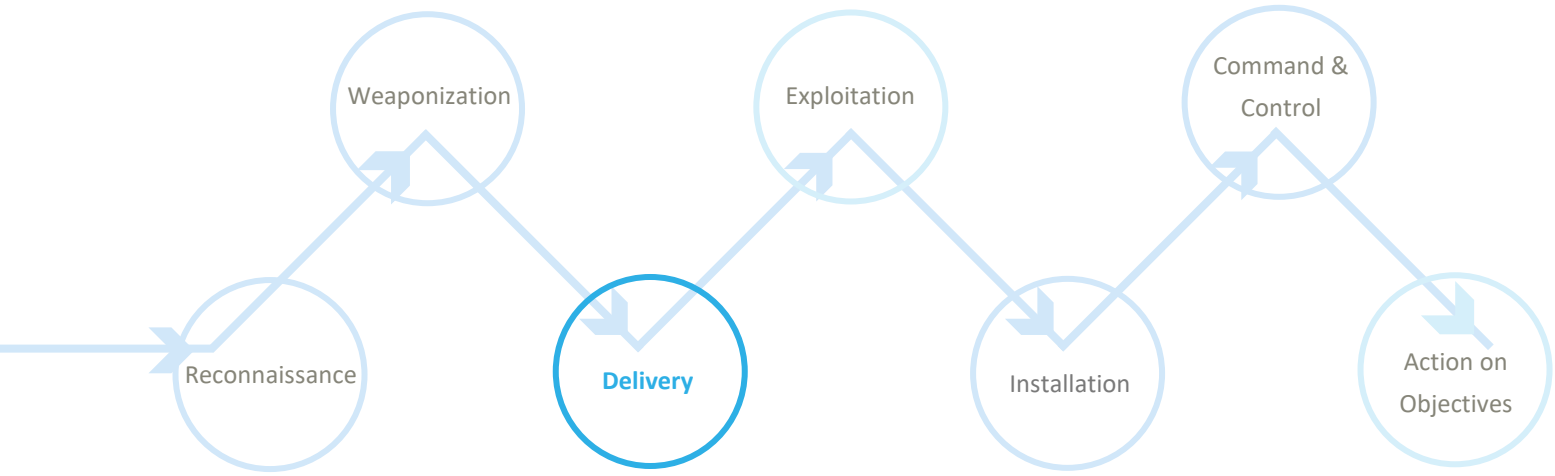
Among others, NÚKIB evaluates cyber incidents on the basis of the MITRE ATT&CK framework, which serves as an overview of known techniques and tactics used in cyber attacks. Among the incidents in May, the "Malicious File" technique prevailed. However, as three of the serious cyber incidents and events that NÚKIB handled in May were caused by insufficient security on the supplier's side, the technique of the month focuses on this issue.

Organisations grant suppliers access to their systems so that they can administer them. For example, suppliers can access their customers' networks via VPN. **Trusted Relationship** is a technique in which attackers abuse supplier accesses to compromise the systems of the intended victims – their clients. If a supplier does not secure access to its clients' networks or secures them worse than access points managed by the organisation itself, for attackers it is the easiest way in. Attackers can also use the technique for supply chain attacks.

MITRE ID: T1199

Mitigation: The first step to mitigate the technique is adequately securing accounts that the suppliers use to access the victim's network. The more robustly secured network accesses the supplier has, the smaller the risk of them being abused. Therefore, organisations should require 2-factor authentication for all remote accesses, follow the principle of the least privilege, and even use whitelisting for the most critical systems. Another preventive step is segmenting the network in such a way that components, which do not require broad network access, are isolated. Organisations should also consider organisational security measures in the form of supplier management, which is described in more detail on page 6.

A representation of "Trusted Relationship" in the Cyber Kill Chain showing at which point attackers use the technique:



Focus on a security measure: Supplier management

In May, NÚKIB handled several serious cases that stressed the need for a supplier management process. In one of the cyber incidents, which caused substantial damage to the attacked organisation, the attacker entered the victim's network through a compromised VPN account of its servicing company. It is unclear now how the credentials leaked from the service company or how the attacker got them. The attacker used them as an access point to the victim organisation and moved from there laterally into other systems.

In the remaining two cases, the organisations themselves discovered poor security processes of their supplier, probably before attackers managed to exploit the weak points. The organisations found out that their information system supplier, among other bad practices, stored their sensitive data in a web-based storage without any authentication mechanism. The evidence so far suggests that nobody has tampered with the data; therefore, NÚKIB registers both cases as cybersecurity events. Nevertheless, the practically non-existent data security would probably be the easiest way to gain and abuse the data.

Obligations associated with supplier management arising from the legislation

Management of suppliers is one of the organisational security measures that subjects regulated by Act No. 181/2014 Coll. on Cyber Security are obliged to perform. The main purpose of the supplier management process is to identify and mitigate the risks associated with the use of third-party services.

Within the scope of supplier management, the above subjects are obliged to lay down rules for their suppliers that take account of the requirements for information security management system, to familiarize their suppliers with these rules and require that they are observed, and manage the supplier-associated risks. Within the scope of human resources security management, obligated persons must ensure familiarizing their suppliers with the security policy and their duties. Within the scope of cybersecurity incident handling, they are obliged to notify about any unusual behaviour of their systems and all suspected vulnerabilities.

The mentioned bodies are also obliged to take account of requirements arising from security measures when choosing a supplier for their information or communication system (so-called significant supplier) and incorporate them into the contract concluded with the supplier. An assessment of risks associated with the fulfilment of the subject matter of the tender shall be performed as a part of all tenders and before concluding a contract. Furthermore, the concluded contracts shall stipulate methods and levels of implementation of security measures, the content of the mutual responsibility for introduction and checking of the security measures, performing regular risk assessment and checking the security measures related to the services provided by either own capacities or with the assistance of a third party (and ensure that the risks and insufficiencies found are addressed). Last but not least, it is necessary to ensure that contracts concluded with suppliers contain relevant parts mentioned in Annex No. 7 to Decree on Cyber Security and regularly review the fulfilment of contracts with significant suppliers with respect to information security management system.

Management of suppliers is a continuous process with many variables. Big suppliers are often in the position where they may determine the conditions for providing their services. At the same time,

the customer has only limited possibilities of incorporating its security requirements into contracts. Similarly, it is not always easy in practice to check the suppliers' approach to ensuring the security of the services supplied by them and whether they observe all measures as declared. But even in such cases, obligated organisations may not resign from their duties to ensure the security of their systems and the data stored in them and have to ensure observance of the fundamental security principles, data protection rules, and the cybersecurity best practice. Among others, it is necessary to communicate with suppliers actively and regularly, require information about the method of provision of the contracted services and immediate rectification of any deficiencies, and strictly enforce fulfilment of contracts. It is also crucial not to be afraid of leaving a supplier that does not provide quality services or not to conclude contracts with a lock-in effect.

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 information use

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.