NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

2021 REPORT ON CYBER SECURITY IN THE CZECH REPUBLIC

2021 REPORT ON CYBER SECURITY IN THE CZECH REPUBLIC

Director's Foreword

Dear reader,

This is the 2021 Report on Cyber Security in the Czech Republic. In the foreword to the previous report, I mentioned the effects of the pandemic on cyber security, including the large-scale shifting of both business and private communication to the Internet. Two years later, the situation has not changed significantly: remote communication has become commonplace or, in some cases, even inevitable. Yet, a further increase in cyberattacks has confirmed that the Internet should be approached with respect and caution.

In 2021, the National Cyber and Information Security Agency (hereinafter the "NÚKIB") had to deal with numerous cyber security challenges and issued two reactive measures, one of them in response to Log4Shell, an extremely severe vulnerability. The NÚKIB also issued the first protective measure in its history.

The approval of the Action Plan for the National Cybersecurity Strategy of the Czech Republic from 2021 to 2025 (the Action Plan) was an important step in strengthening Czech cyberspace. The Action Plan sets out specific steps to achieve the goals and visions of the National Cyber Security Strategy. It reflects our strategy based on society-wide approach and the need for cooperation across the public sector, private sector, and academia since efficient cooperation is essential for cyberspace protection. We are all interconnected in cyberspace; therefore it is up to each one of us to help protect it.

We analysed threats and sought to act preventively throughout the year. We helped address the consequences of cyberattacks when necessary. We also attended many events in the Czech Republic and abroad, and organised trainings, seminars, and conferences in collaboration with public, domestic, and foreign partners. We enhanced international cooperation, supporting research and development in the field, and developed cooperation with partners from the private sector.

We did all this and much more with the help of our partners and the public to strengthen the security and resilience of the Czech Republic in cyberspace.

Considering the release date of this Report, I cannot fail to mention the aggressive war that the Russian Federation has unleashed in Europe. It is something most of us could not imagine until recently. Although it is too early to evaluate all of its consequences, one thing is certain: the security environment we lived in over recent years is changing radically, and the effects of these changes will impact cyberspace. The need to strengthen our capabilities and capacity is even more pressing now, as is the need for a sufficient number of highly skilled professionals. We must build a secure and resilient information infrastructure. We must prepare and educate our fellow citizens. And we must do this quickly.

Cooperation in protecting cyberspace is increasingly important. I would like to thank the 283 organisations that participated in the preparation of this 2021 Report on Cyber Security in the Czech Republic by filling out our questionnaire. Cyber threats can only be faced with partners by your side, and we appreciate your trust and support.

Karel Řehka

Summary of the 2021 Report on Cyber Security in the Czech Republic

- The year 2021 was marked by **an increase in malicious cyber activities** throughout the Czech Republic. The number of cyber incidents registered by the NÚKIB and CSIRT.CZ grew compared to the previous year. According to the Police of the Czech Republic, cybercriminal activities also showed an increasing trend.

- Compared to the 99 incidents in 2020, 157 cyber security incidents were reported to the NÚKIB in 2021. The number of incidents reported by non-regulated entities also grew compared to last year. This increase was likely caused by NÚKIB's proactivity, greater awareness of NÚKIB activities, and the severity of incidents that entities faced. The most frequent types of attack in 2021 included **phishing, scam emails, and external network scanning.**

- In 2021, the most serious cyber threats in the Czech Republic included **newly published vulnerabilities, ransomware attacks, and phishing or spear-phishing**. Czech institutions and companies were mainly affected by ProxyLogon, ProxyShell, and Log4Shell, which caused nearly one fifth of all the incidents registered by the NÚKIB. There was also a significant increase in ransomware attacks, many involving RaaS (ransomware-as-a-service). As in previous years, phishing attacks were among the most frequent attack vectors. Phishing became increasingly sophisticated in the past year.

- In 2021, the NÚKIB issued **26 alerts** in reaction to current threats. Moreover, the NÚKIB issued **two reactive measures** in connection with Microsoft Exchange Server and Log4Shell vulnerabilities. For the very first time, the NÚKIB also issued a **protective measure** with the aim to secure the communication of administrators and operators of information systems.

- In cooperation with the Ministry of Foreign Affairs and under the auspices of the Czech Government, the NÚKIB organised **the 3rd Prague 5G Security Conference**, which focused on issues associated with the security of 5G networks and emerging and disruptive technologies (EDTs).[1] Almost 70 speakers from Europe and other parts of the world (e.g. Israel, Korea, Japan, Australia, the USA, Canada, and India) spoke at the conference. The two-day conference was divided into several thematic virtual panels attended by hundreds of international spectators. At the conclusion of the conference, the NÚKIB introduced **Prague Proposals on Cyber Security of EDTs** and the **Prague Proposals on Telecommunications Supplier Diversity.**

- In 2021, the NÚKIB continued training civil servants. Over 26,500 users completed e-learning courses **Dávej kyber!** (Get Cyber Skilled!) and **Šéfuj kyber!** (Manage Cyberspace!). More than 2,800 users graduated in the foundations of safe behaviour on the Internet through a course called **Bezpečně v kyber!** (Stay Safe in Cyberspace!). More attention has been given to the education of healthcare staff. The NÚKIB launched an e-learning course called **Kyber nemocnice!** (Cyber Hospital!), attended by more than 4,400 employees. As in previous years, numerous **educational activities for children, youth, and the broader public** took place last year.

- The year 2021 saw a return to in-person cyber exercises with a total of 14 such events taking place on the national and international level. Among other things, the NÚKIB organised **Health Czech**, the very first cyber security exercise for the healthcare sector. In terms of international exercises, the Czech team earned 3rd place in **the Locked Shields 2021** exercise, a particularly noteworthy achievement.

[1] EDTs include, for example, artificial intelligence, quantum technologies, autonomous systems, and Massive Internet of Things.

Table of Contents

List of Abbreviations

ACS – Act on Cyber Security
AFCEA – Armed Forces Communications & Electronics Association
CII – Critical information infrastructure
CIWFC – Cybernetic and Information Warfare Forces Command
CR – Czech Republic
CSD – Cyber Security Decree
DoS/DDoS – Denial of Service/Distributed Denial of Service
EDTs – Emerging and Disruptive Technologies
ENISA – European Union Agency for Cybersecurity
EU – European Union
FREAK – Factoring RSA Export Keys
INCD – Israel National Cyber Directorate
ITU – International Telecommunication Union
JCU – Joint Cyber Unit
NATO – North Atlantic Treaty Organisation
NIS – Network and Information Security
NÚKIB – National Cyber and Information Security Agency
OECD – Organisation for Economic Co-operation and Development
OEWG – Open-Ended Working Group
OSCE – Organisation for Security and Co-operation in Europe
RaaS – Ransomware-as-a-Service
SIEM – Security Information and Event Management
SSL – Secure Sockets Layer
TLS – Transport Layer Security
UN – United Nations
VoIP – Voice over Internet Protocol

2021: Cyber Security in the Czech Republic in Figures

476
cyber incidents reported to the NÚKIB

157
cyber incidents handled by the NÚKIB

8
significant cyber incidents handled by the NÚKIB

1,726
security incidents handled by CSIRT.CZ – the National CSIRT of the Czech Republic

1,281
phishing attacks handled by CSIRT.CZ

9,518
cybercrimes and crimes committed on the Internet

490
participants of cybersecurity trainings organised by the NÚKIB

14
cybersecurity trainings organised by the NÚKIB

33,839
users trained in courses organised by the NÚKIB

60
critical information infrastructure entities

131
critical information infrastructure (CII) information and communication

162
administrators and providers of important information systems

379
important information systems

124
operators of essential service

147
essential services information systems

About the Report

At the beginning of 2022, the NÚKIB sent a questionnaire with 79 questions to entities regulated by Act No 181/2014, on cyber security and on amendments to related laws (Act on Cyber Security), as amended (hereinafter the "ACS"), as well as to many other key institutions and organisations not regulated by the ACS. The questions covered a broad range of topics such as cyberattacks, cyber security costs, cyber security staff, users, technologies, and implemented processes. The questionnaire was filled in by 283 entities. Of this total, 199 entities were regulated by the ACS; the remaining 84 were not regulated. The NÚKIB drew information from these materials for the 2021 Report on Cyber Security in the Czech Republic (hereinafter the "Report"). All of the data obtained from the questionnaires were anonymised.

Evaluation Process

Our assessment of the state of cyber security in the Czech Republic is based on an analytical process consisting of the evaluation of questionnaires, the findings of the NÚKIB, information provided by partners, and other available information from verified sources. The NÚKIB was not able to check the data provided by the respondents or to verify their claims. The analytical conclusions contained in this report are based on the premise that the answers in the questionnaires were not distorted. The analytical assessment is described using expressions of likelihood (see below). The Report on Cyber Security in the Czech Republic does not provide an exhaustive list of cyber security activities. The goal of this document is to describe and assess the threats in cyberspace that the Czech Republic faced in 2021 and the actions taken to mitigate them.

Expressions of likelihood used in the 2021 Report on Cyber Security in the Czech Republic

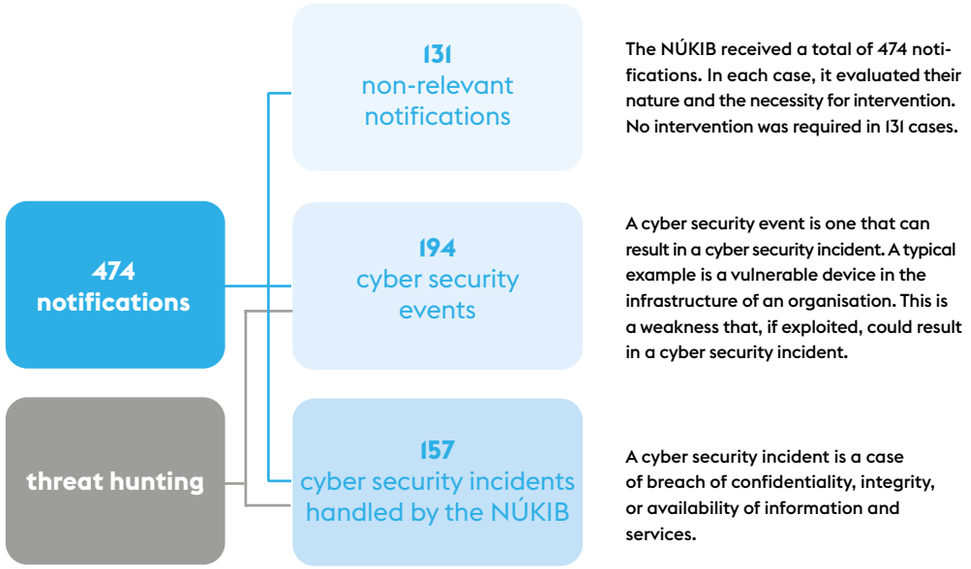
Expressions of likelihood and their percentage values:

Expression	Likelihood
Almost certain	90–100 %
Highly likely	75–85 %
Likely	55–70 %
Cannot be ruled out/Realistic possibility	25–50 %
Unlikely	15–20 %
Highly unlikely	0–10 %

Cyber Security in the Czech Republic in 2021 [2]

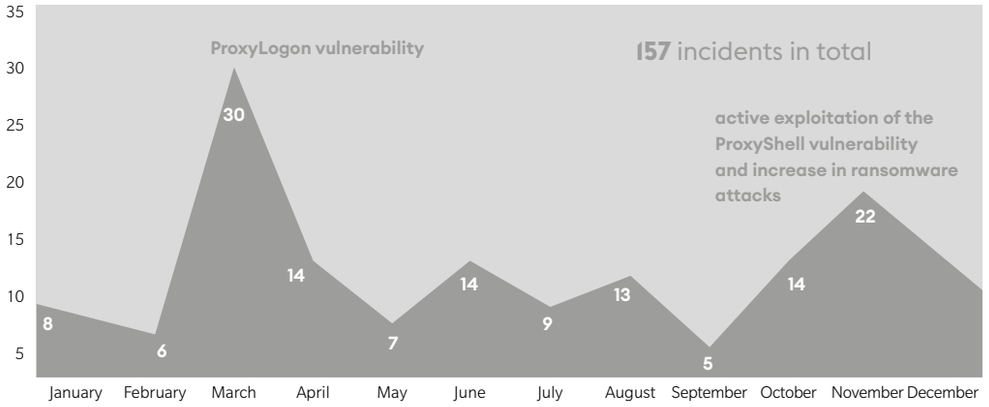
Number of Cyber Security Incidents Registered by the NÚKIB in 2021

In 2021, the NÚKIB received 474 notifications, the majority of which were categorized as cyber security incidents. **The NÚKIB handled a total of 157 cyber security incidents in 2021 based on external notifications and proactive threat hunting.**



March set a new record with 30 incidents; by then, the ProxyLogon vulnerability aimed at compromising the widely used Microsoft Exchange Server service was being massively exploited. The second-busiest month was November, which saw active exploitation of the ProxyShell vulnerability in the same service throughout the Czech Republic and an increased number of ransomware attacks.

Graph 1: **Number of incidents handled in 2021**



[2] This information is based on NÚKIB resources and results of 283 questionnaires (see 'About the Document' above).

The number of incidents reported by non-regulated entities has grown compared to the preceding year. While they accounted for one third of the handled incidents in 2020, the ratio increased to 40% in 2021. The number of incidents reported by non-regulated entities has likely (55%–70%) grown due to to greater general awareness of the NÚKIB's activities and the severity of individual incidents. Nonregulated subjects prevailingly notified the NÚKIB of ransomware attacks that affected their operation.

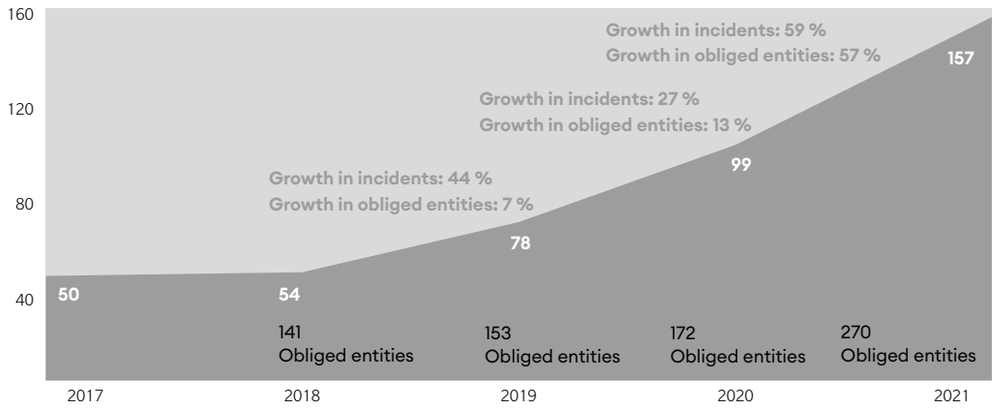
Regulated entities	Non-regulated entities
94 incidents	**63** incidents

Comparing the Number of Incidents with Preceding Years: Growth Due to Several Factors

The number of incidents detected by the NÚKIB has been continuously growing. In 2021, the NÚKIB handled 157 incidents, **an increase of 59% compared to the preceding year** with 99 incidents. The increase is likely (55%–70%) caused by several factors, the first and most important one being the increasing number of regulated entities. As the number of obliged entities grows, so does the number of cyber incidents reported by those entities. Nevertheless, the number of obliged entities is not the only factor affecting the number of incidents, as evident from Graph 2. The number of incidents is growing faster than the number of obliged entities. Key factors also include increased activity of attackers, including ransomware attacks by cybercriminal groups, and the NÚKIB's proactive searching for attacked stations.

It is highly likely (75%–85%) that the number of cyber security incidents will continue to grow in the coming years. The number of obliged entities will further increase with the upcoming amendment to the EU NIS Directive.[3] Given the financial profitability of attacks, the activity of cybercriminal attackers will likely (55%–70%) continue to increase.

Graph 2: **Relation between the growth in incidents and obliged entities by year** [4]



[3] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. For more information about the draft amendment to this Directive, see the International Cooperation section.

[4] The percentage growth is always related to the preceding year.

Classification of Cyber Incidents Reported to the NÚKIB [5]

The classification has largely reflected the preceding year's trends in ransomware attacks and vulnerability exploitation:

1. Availability: The majority of the preceding year's incidents negatively impacted availability of services. They included DDoS attacks, technical faults, and ransomware attacks that limited operations of the attacked organisations due to inadequate backup solutions.

2. Malicious code: This was the second-most-frequent category. Most incidents in this category were caused by ransomware attacks. Nevertheless, they did not cause significant damage since the attacked organisations had appropriate backup solutions. This enabled them to resume operations quickly, and the availability of their services was not affected. Aside from ransomware attacks, the NÚKIB also handled cases of malware with control servers in Czech territory (mainly TrickBot, Emotet, and Dridex).

3. Intrusions: The number of incidents that NÚKIB classified as intrusions has also significantly increased compared to 2020. Last year, intrusions accounted for 9% of all incidents; this year, the figure rose to 22%. While malicious code and incidents targeting availability of services occurred steadily throughout the year, intrusions sharply increased when information about new vulnerabilities was released, such as during the March MS Exchange Server vulnerability exploitation campaign.

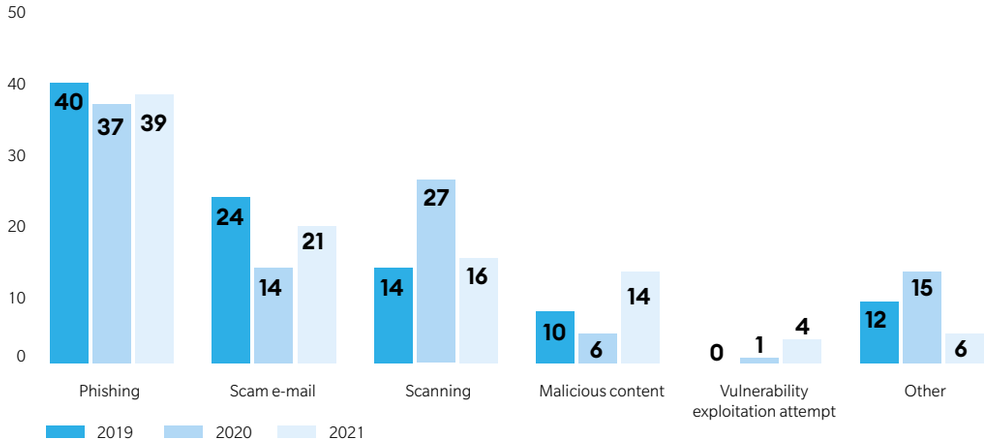
	Percentage of incidents 2020	Percentage of incidents 2021	Trend during the year
Availability availability disruption caused by DoS/DDoS attacks or sabotage	29%	34%	
Malicious code viruses, worms, Trojan horses, dialers or spyware	36%	25%	
Intrusions compromising an application or user account	9%	22%	
Fraud phishing, identity theft or unauthorised use of ICT	15%	10%	
Information Content security unauthorised data access, unauthorised data modification	4%	8%	
Intrusion attempts attempts to abuse vulnerabilities or login attempts	4%	1%	
Information Gathering scanning, sniffing, social engineering	2%	0%	

[5] Cyber-incident classification is based on the ENISA taxonomy: Reference Incident Classification Taxonomy — ENISA. The "Abusive Content" and "Other" categories have been left out from the table above since none of them was represented among incidents over the last two years.

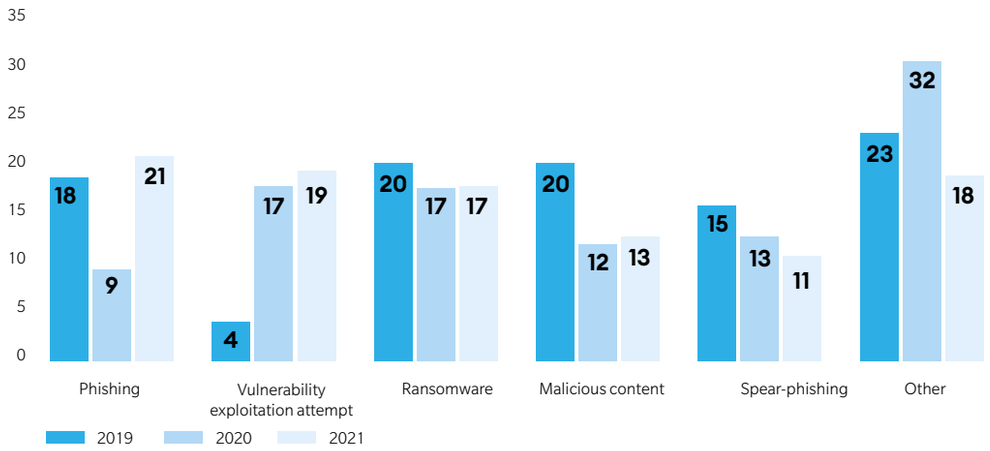
Incidents from the Perspective of Entities: Increasingly Severe Cases of Phishing and Vulnerability Exploitation

The most frequent types of cyberattacks that surveyed institutions and organisations encountered in 2021 included phishing, scam emails, and external network scanning (Graph 3).[6] Similarly to preceding years, the most frequently detected attacks included technically simpler types of attacks that are easier to detect. **According to the respondents of our questionnaire, the most serious types of attack in 2021 were phishing, attempts to exploit vulnerabilities, and ransomware** (Graph 4). While ransomware has long been among the types of attack that entities perceive as the most serious, phishing and attempts to exploit vulnerabilities came to the fore in 2021. The change in the perception of the severity of these types of attacks is likely (55%–70%) affected by the increasing sophistication of phishing attacks and the more frequent exploitation of vulnerabilities by threat actors (for more details, see the Cyber Threats and Threat Actors section). **Nearly three quarters of respondents recorded a cyberattack attempt in 2021, yet the attacks only succeeded in breaching data confidentiality, integrity, or availability in one quarter of cases** (Graph 5). The number of recorded incidents ranged between one and five in most of the affected entities.

Graph 3: **Categories of the most common types of cyberattacks 2019–2021** (%)

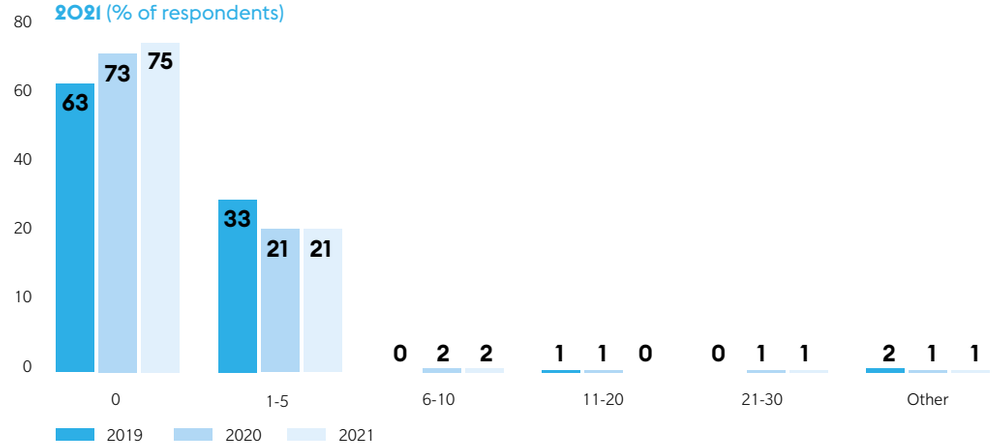


Graph 4: **Categories of the most serious types of cyberattacks 2019–2021** (%)



[6] The sum of the percentages in the graphs may not be 100 due to the rounding of the data obtained through the questionnaires.

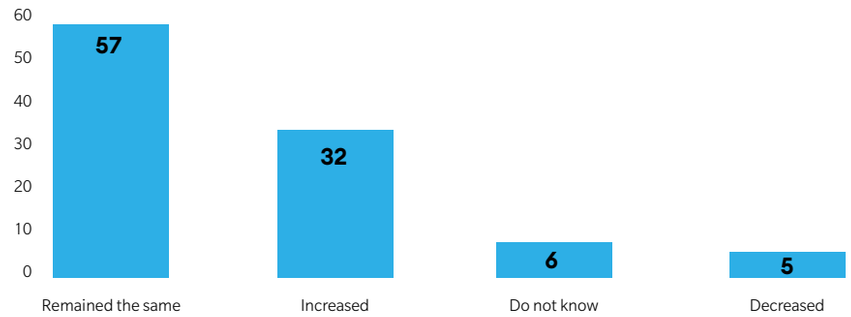
Graph 5: **Percentage of attacks involving a breach of data confidentiality, integrity, or availability in 2021** (% of respondents)



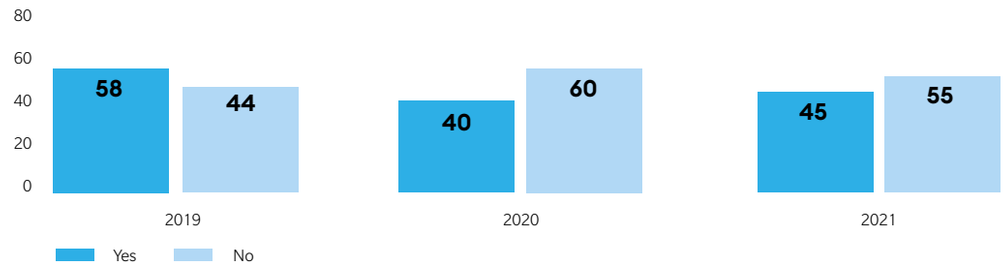
Cyber Security Funding: Much Needed, although Moderate Budget Increases

While the cyber security budget remained about the same as last year for over a half of the respondents, almost one third saw an increase (Graph 6). **This is a significant improvement compared to 2020**, which was affected by the pandemic, with funds allocated to cyber security decreasing in 43% of cases. **Despite this, more than half the respondents consider the funds allocated to cyber security to be insufficient** (Graph 7). Like in the preceding years, the percentage of funds spent on cyber security in 2021 ranged between 0% and 5% of the overall budget for most of the respondents (Graph 8).

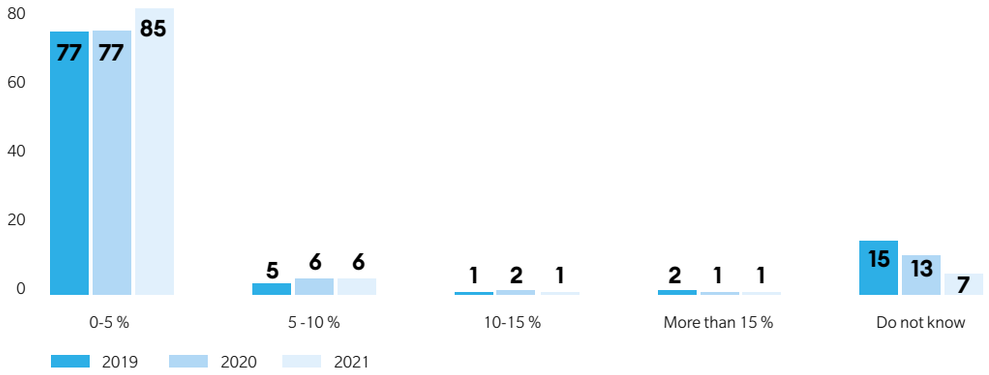
Graph 6: **Trend in respondents' budgets allocated to cyber security compared with 2020** (%)



Graph 7: **Did the respondents consider the funds allocated to cyber security between 2019 and 2021 sufficient?** (%)



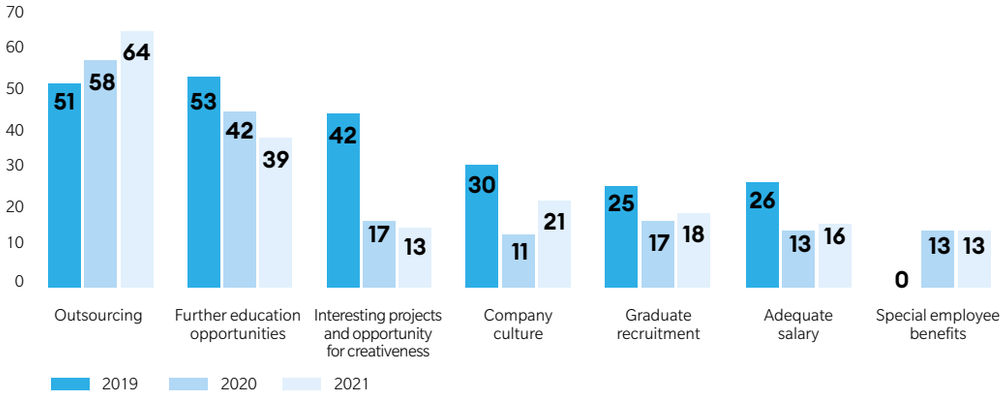
Graph 8: **Share of the organisation's total budget allocated to cyber security between 2019 and 2021** (% of respondents)



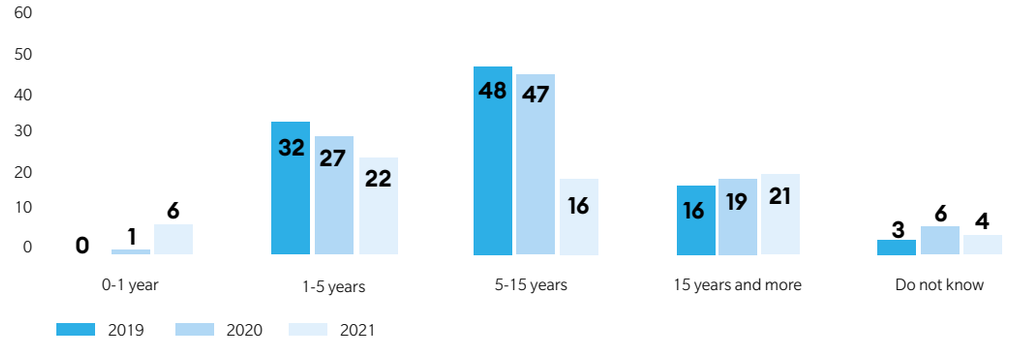
People as Experts: Low Salaries and Increasing Numbers of Entry-Level Employees

Hiring cyber security experts is a critical challenge facing many Czech organisations. In this respect, the high demand for experts and the high salary expectations associated with it are the main issues. **Nearly three quarters of the respondents said that low salary is the key factor discouraging job applicants in cyber security**. Many organisations do not have sufficient funds to pay the experts they need, and hence are forced to solve the situation by means other than competitive salaries. **Almost two thirds of respondents facing skill shortages solve their situation by outsourcing.** Other respondents try to attract and keep cyber security staff through various company benefits, such as the possibility of further education and participation in interesting and promising projects (Graph 9). **Although the number of organisations filling vacancies by hiring graduates remained roughly the same as the preceding year, the number of employees with less than one year of experience rose in 2021** (Graph 10). This possibly indicates that entities have begun hiring employees for cybersecurity positions from unrelated fields.

Graph 9: **How did the organisations seek to address the lack of cyber security experts between 2019 and 2021?** (%)



Graph 10: **Average relevant work experience of employees providing cyber security in the respondents' organisations** (%)



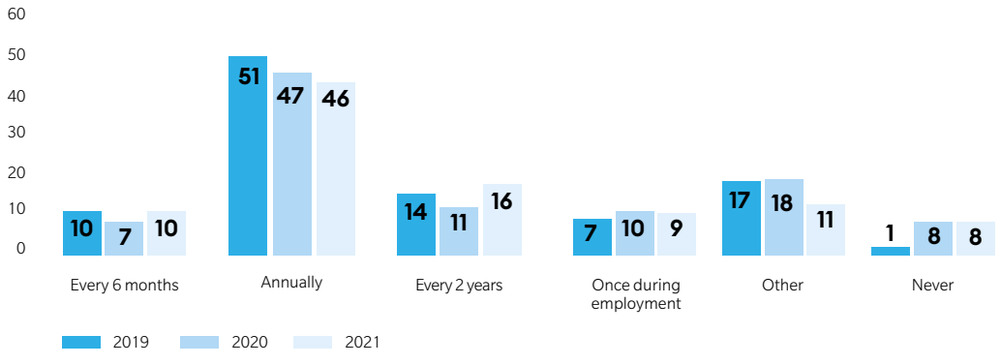
One positive factor is that salaries do not significantly affect the fluctuation of cyber security experts. In 2021, only 15% of the respondents had one or more of their cyber security experts leave (Graph 11), while their salary was not the main reason for leaving in 75% of the cases. It cannot be ruled out (25%– 50%) that the reason for such a low number of employees leaving was a low number of dedicated cyber security experts in the respondents' institutions and companies.

Graph 11: **How many cyber security employees left your organisation within 12 months from their hiring in 2021?** (%)

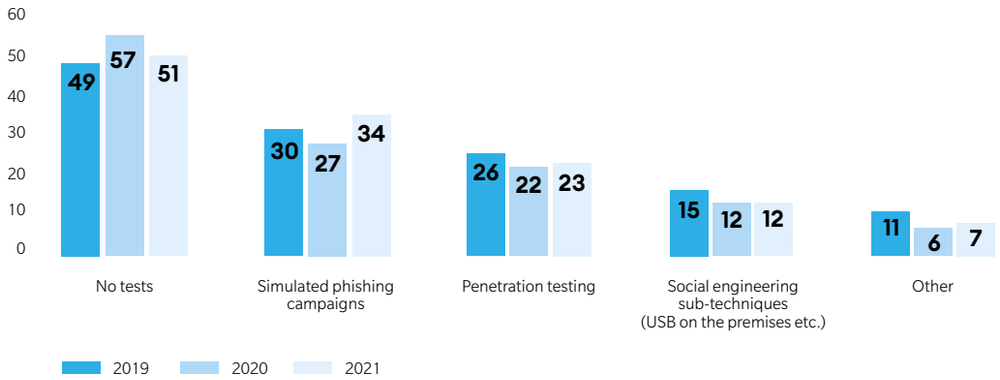
People as Users: Training and Testing Employees' Resilience

As part of bolstering their cyber security, most Czech institutions also focus on one of its crucial elements: users. **Up to 86% of respondents train users in cyber security and familiarise them with current cyber threats.** Training is often held annually (Graph 12), and about two thirds of the organisations use internal training or e-learning. **At the same time, nearly half of the organisations try to improve their employees' resilience to cyber threats.** Resilience testing is often performed through simulated phishing campaigns, penetration testing, or social engineering sub-techniques (Graph 13).

Graph 12: **Frequency of cyber security training for users in organisations between 2019 and 2021** (% of respondents)



Graph 13: **Forms of testing of employees' resilience to cyber threats in organisations between 2019 and 2021** (% of respondents)



Cyber Threats and Threat Actors

Vulnerabilities in 2021: The Cause of Nearly One Fifth of All Incidents

In 2021, newly published vulnerabilities significantly affected cyber security in the Czech Republic and abroad. **Cyber security incidents handled by the NÚKIB mainly involved the ProxyLogon, ProxyShell, and Log4Shell vulnerabilities, which accounted for nearly 18% of all incidents registered by the NÚKIB in 2021.** These vulnerabilities are particularly serious. The systems they affect are used worldwide, and it is not technically challenging to exploit them. Attackers can use them for a myriad of purposes, including completely compromising servers. Our respondents also noticed a high rate of vulnerability exploitation. As many as 40% of organisations detected an attempt to abuse a vulnerability, an increase of 14% compared with 2020.

The number of incidents associated with vulnerabilities reported to the NÚKIB in 2021:

21	5	2
ProxyLogon	ProxyShell	Log4Shell

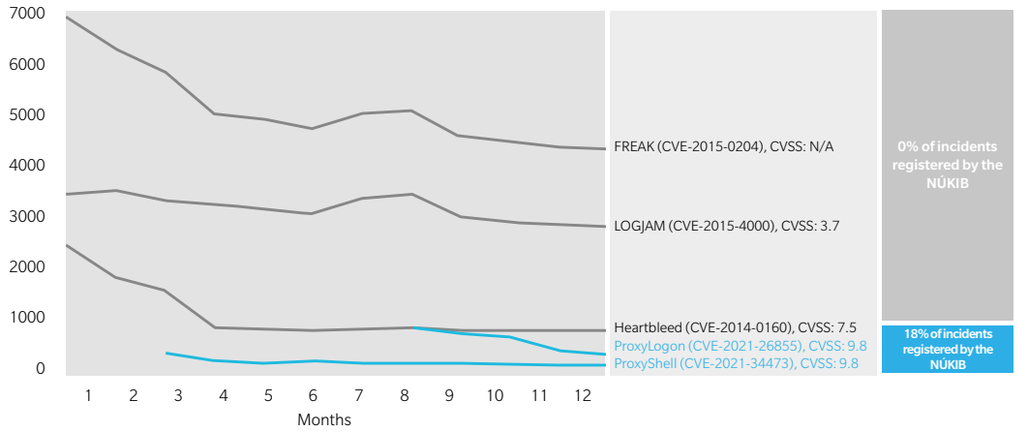
In March, the ProxyLogon vulnerability exploitation campaign, during which attackers compromised Microsoft Exchange email servers, affected 21 Czech organisations, 11 of them in the public sector. Several of these cases were also mentioned in the media; one such case affected the systems of the city of Prague.[1] Following the NÚKIB's alert, Prague City Hall discovered attacked servers, which it immediately disconnected and replaced with clean installations. The incident limited the availability of the email server; according to publicly available information, no data were lost.

ProxyLogon is a set of vulnerabilities affecting Microsoft Exchange Server. It was published on 2 March 2021. ProxyLogon enables access to email boxes on a server and the subsequent launching of code without authentication and user interaction. Microsoft Exchange email servers are a tempting target for attackers as Microsoft Exchange Server is one of the most common mail servers in the world, used by both large companies and state organisations. By their nature, they contain a lot of sensitive information which, if compromised, attackers can use for espionage or as an entry point into an organisation's network.

As shown in Graph 14, **by the end of the year the exploited ProxyLogon, ProxyShell, and Log4Shell vulnerabilities were not the most widespread in the Czech Republic**. According to the Shodan tool, most devices in the Czech Republic are vulnerable to three older vulnerabilities, namely FREAK, LOGJAM, and Heartbleed. Nevertheless, no organisation reported an incident associated with these vulnerabilities to the NÚKIB in 2021, perhaps because all three vulnerabilities affect old versions of cryptographic protocols (SSL/TLS contained in OpenSSL versions older than 1.0.1k). These versions do not meet the recommendations of the NÚKIB,[7] and hence entities obliged by the ACS should not use them in their infrastructure.

[7] See the document Minimum requirements for cryptographic algorithms.

Graph 14: **2021 Vulnerability trends in the Czech Republic** [8]



The Log4Shell vulnerability published on 9 December was not significantly manifested in the incidents reported to the NÚKIB. Considering the widespread nature of this vulnerability and its massive exploitation, more organisations may have been affected than the number the NÚKIB registered. Nevertheless, the impacts of Log4Shell were not as extensive as expected given the severe nature of this vulnerability.[ii]

The **Log4Shell** vulnerability is contained in the Log4j log tool used in hundreds of systems and applications. By the time the vulnerability was discovered, the total number of vulnerable systems was estimated at many hundreds of millions around the world. The vulnerability means it is possible to attack systems that are not directly accessible from the Internet, launch code without any authentication, and thus gain overall control of the server. Consequently, attackers can gain access details, read and exfiltrate data, and install other malicious code, including ransomware. This can all be done with relatively little effort since exploiting this vulnerability is not technically challenging.

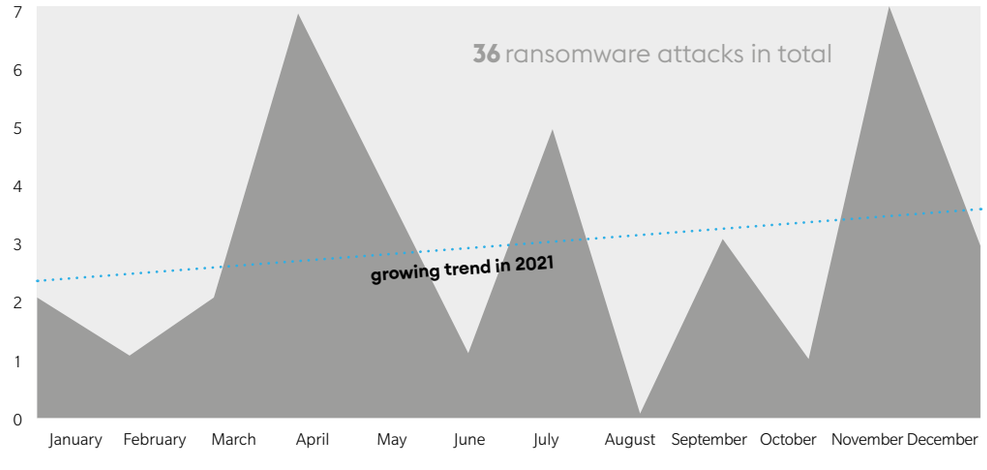
The Most Frequent Technique in 2021: Exploiting Applications Open to the Internet

The technique that attackers most often used in the incidents registered by the NÚKIB in 2021[9] **was Exploit Public-Facing Application**.[iii] This technique also relates to a series of Microsoft Exchange ProxyLogon and ProxyShell vulnerabilities, where the servers are accessible on port 443 and hence open to the Internet. It confirms that these vulnerabilities played a significant role in Czech cyber security in 2021.

Ransomware-as-a-Service: Increased Activity and Change of Modus Operandi

The NÚKIB addressed 36 ransomware attacks in 2021, an increase of 71% compared with the preceding year which saw 21 ransomware incidents. The growing trend in ransomware attacks continued in 2021 with their number increasing by about one quarter over the last 12 months (Graph 15). Most ransomware incidents occurred in April and November. In April, ransomware attacks accounted for half of all cyber incidents reported to the NÚKIB during the entire year.

Graph 15: **Number of ransomware attacks registered by the NÚKIB in 2021**[10]



Although the NÚKIB registered significant growth in ransomware attacks, individual entities saw an 11% decrease of this type of attack or attack attempt. **This might indicate that this type of attack is increasingly targeted and effective. Nevertheless, other factors may also play a role.** For example, the number of incidents reported by non-regulated entities increased in 2021, and ransomware attacks accounted for a significant share of the reported incidents.

The ransomware-as-a-service (hereinafter "RaaS") phenomenon has been on the rise in recent years. Cybercriminal groups offer RaaS as a products for purchase to anyone who wants to carry out a ransomware attack. The offered services differ based on the type of ransomware and the amount charged for the service. A service package can include 24/7 user support and information about the current state of infection and the number of encrypted files.[iv]

One typical feature of RaaS in 2021 was 'double extortion', which means that attackers both encrypt and exfiltrate the files of their victims. They then threaten their victim that the data will be published and re-sold if they do not pay the ransom. **Among the incidents handled by the NÚKIB, double extortion was associated with 14% of ransomware attack victims.** In one attack handled by the NÚKIB in 2021, the attackers even used triple extortion, with the ransomware operators encrypting the data, exfiltrating them, and then threatening the victim not only with the publication of the data but also with a DDoS attack (see the box below).

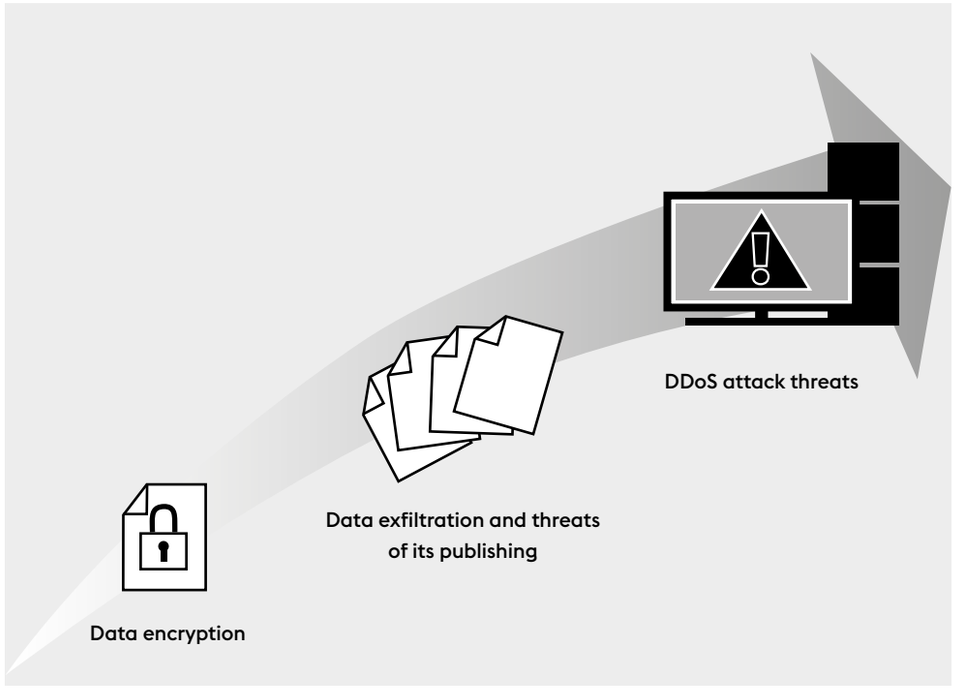
[8] The data were obtained from the Shodan tool. The Log4Shell vulnerability is not included in the graph because tools such as Shodan do not register it as scanning for this vulnerability would be so intrusive that it would become a de facto incident.

[9] The NÚKIB evaluates cyber incidents based on the MITRE ATT&CK framework, which serves as an overview of known techniques and tactics used in cyberattacks. The NÚKIB also uses it to determine how often attackers use the techniques and tactics in their attacks.

[10] This graph is only based on the incidents reported to the NÚKIB. Thanks to darkweb monitoring, the NÚKIB is aware of other Czech victims of ransomware groups.

In April, the Avaddon ransomware encrypted the networks of the City of Olomouc. According to the information provided by the municipal authority, the attackers entered the infrastructure through its element asccessible from the Internet. Before encrypting the data, they exfiltrated them and then demanded the municipal authority pay a ransom of USD 100,000. When the municipal authority did not pay the ransom, the attackers published the data on their darkweb pages. The information included contact details from payments for municipal waste and information about the authority's employees. When the municipal authority did not react to the threats, the attackers tried to exert additional pressure and commenced DDoS attacks against the authority's systems. The extortion and attacks lasted more than a month, and the municipal authority estimated the damage at about CZK 1,000,000 immediately after the attack.[v]

Scheme of triple extortion ransomware



Phishing, Spear-Phishing, and Scam Emails: The Most Frequent Attack Vectors Show Increasing Sophistication

In 2021, 90% of the respondents experienced phishing emails, 47% experienced spear-phishing emails, and 84% experienced scam emails. Phishing is one of the most frequent attack vectors, as shown by the regularity of its occurrence among the incidents reported to the NÚKIB. The NÚKIB registered no phishing, spear-phishing, or vishing campaign in only three months in 2021.

In reaction to phishing campaigns, the NÚKIB issued two alerts in 2021. In one of the campaigns, the attackers tried to lure users into clicking on a scam link and filling in their login details, allowing them to exploit the mailbox to spread the phishing further.

- **Alert regarding a new wave of extortion scam emails**
- **Alert regarding a new wave of phishing emails**

Another two alerts were issued by the NÚKIB in connection with waves of scam phone calls (vishing), in which the attackers pretended to be a bank or Microsoft technical support employees.

- **Alert regarding scam phone calls from fake Microsoft technical support**
- **Alert regarding vishing abusing the identity of bank institutions**

https://www.nukib.cz/cs/infoservis/hrozby/1670-upozorneni-na-novou-vlnu-podvodnych-vyderacskych-emailu/
https://www.nukib.cz/cs/infoservis/hrozby/1680-upozornujeme-na-novou-vlnu-phishingovych-mailu/
https://www.nukib.cz/cs/infoservis/aktuality/1699-upozorneni-na-podvodne-telefonaty-od-falesne-technicke-podpory-microsoft/
https://www.nukib.cz/cs/infoservis/hrozby/1705-upozorneni-na-vishing-zneuzivajici-identitu-bankovnich-instituci/

90 %
of the surveyed organisations claimed that they faced a **phishing attack** or attempt in 2021

84 %
of the surveyed organisations claimed that they faced an **scam email attack** or attempt in 2021

47 %
of the surveyed organisations claimed that they faced a **spear-phishing attack** or attempt in 2021

11 %
of the surveyed organisations claimed that they faced a **vishing attack** or attempt in 2021

Phishing attacks get more and more sophisticated every year. In recent years, phishing emails have already begun to show a good command of the Czech language, more elaborate formats, and varying motifs (such as executor notices, minutes of meetings, and topics related to COVID-19).[vi] **In 2021, some attackers employed a two-phase plan in an effort to expand the reach and increase the efficiency of their attacks.** In the first phase, they sent phishing emails with forged sender addresses, requiring the user to click on a link or open an attachment. When the attack was successful, the attackers exploited the compromised email addresses in the second phase to send phishing emails to compromise other institutions and organisations. In some cases, the phishing emails built upon preceding email communication with the victim.

Supply Chain Attacks: Varying Perceptions of a Serious Threat

In 2021, the international scene witnessed numerous major supply chain attacks. **One of the most significant was the ransomware attack on the Kaseya supply chain** (see the box below) **which, despite its large scope, was not among the incidents registered by the NÚKIB**. Still, one cyber incident involving a ransomware attack on a server of a Czech company providing ICT solutions should be noted. This attack resulted in the loss of data of all the clients using the attacked server, including the backups. Based on the information available, we cannot say whether the attacker directly aimed at the data of the company's clients or only at the supplier's server and the clients were only secondary victims of the attack.

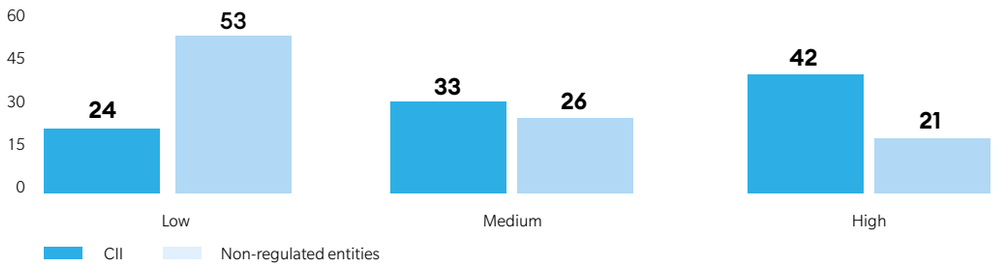
Ransomware attack on Kaseya

The biggest supply chain ransomware attack so far occurred in July 2021, when ransomware gang REvil attacked Kaseya, a software solutions supplier. The attackers exploited a vulnerability to compromise the Kaseya VSA software used by Managed Service Providers (MSPs). REvil compromised hundreds of MSP servers, from which the ransomware spread to their clients. In total, the systems of more than 1,500 companies in 18 countries were attacked.

A supply chain attack or attempt was detected by approximately 6% of institutions and organisations in 2021. Although this is a twofold increase compared with 2020, this type of attacks remains less frequent. This is likely (50%–70%) because of a combination of several factors, such as the low incidence of this type of attacks in the Czech Republic, the frequent inability of organisations to detect such attacks, and the attackers' efforts to remain unnoticed in the victims' systems.

The reason why most entities perceive this threat as low is likely (55%–70%) the long-term low incidence of registered supply chain attacks. Nevertheless, the perception of this threat differs depending on the category to which the entity belongs. While most non-regulated entities perceive this threat as low, **approximately three quarters of the obliged entities involved in critical information infrastructure perceive it as medium or high** (Graph 16).

Graf 16: **How serious was the threat of cyberattacks from service, software and hardware providers in 2021?** (% of respondents from CIIs and non-regulated entities)



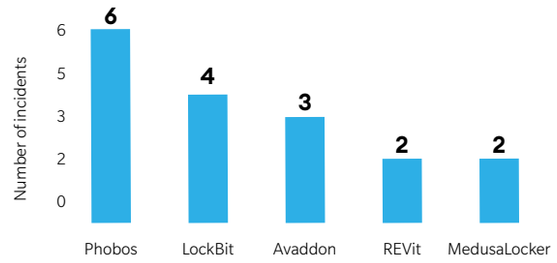
Cyber Threat Actors

Cybercrime and activities of state-sponsored actors in cyberspace are among the most severe long-term cyber security threats in the Czech Republic.

State-sponsored groups are usually highly sophisticated actors employing a broad range of techniques to achieve their goals. They continue to improve their tools over time. **In recent years, these groups have begun using open-source tools for their attacks more and more frequently, focusing on the active exploitation of zero-day vulnerabilities**.[vii] This trend also continued in 2021.[viii] We cannot rule out (25%–50%) that some of the incidents handled by the NÚKIB which were associated with newly published vulnerabilities were carried out by state-sponsored groups.

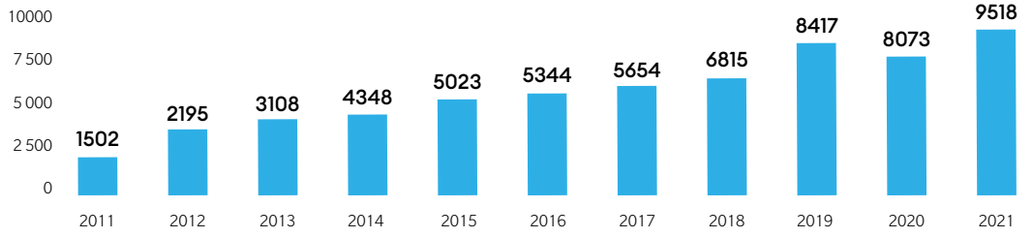
In 2021, cybercriminal groups primarily focused on various types of fraud, including recurring waves of scam emails and other messages or investment fraud.ix Ransomware gangs accounted for a significant share of cybercrime, with a noticeable trend of shifting towards the RaaS model. **All types of ransomware that were most frequently present among the incidents registered by the NÚKIB are offered as a service** (Graph 17). It is likely (55%–70%) that the RaaS model will continue to prevail in attacks on Czech institutions and organisations in the coming year.

Graph 17: **The most active ransomware groups in the CR**



Statistics from the Police of the Czech Republic show that the number of cybercrimes and crimes committed on the Internet has been growing over the long term (Graph 18). The upward trend was disrupted by an amendment to the Criminal Code in 2020, which increased the damage threshold for categorisation as a criminal offence. In total, 9,518 offences falling under the categories of cybercrime and other crimes committed in cyberspace were recorded in 2021, a year-on-year increase of 18%. Based on the developments so far, it is highly likely (75%–85%) that the number of offences committed on the Internet will continue to grow in the coming years.

Graph 18: **Cybercrime cases investigated in the CR between 2011 and 2021**



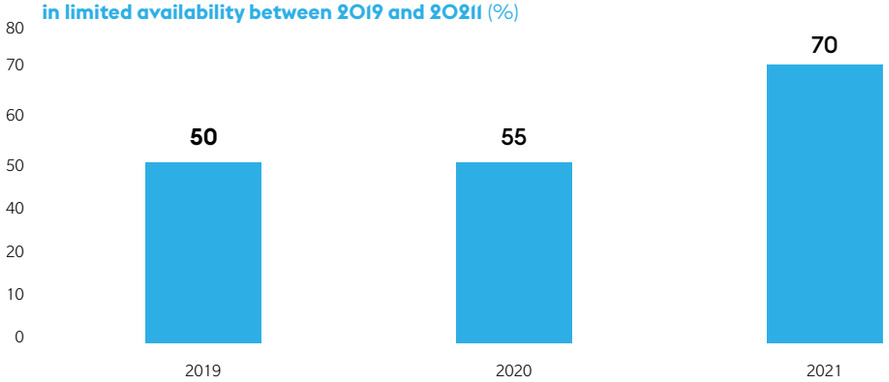
source: Police of the Czech Republic

Targets of Cyberattacks

Critical Information Infrastructure: Utmost Need to Ensure Service Availability

As in preceding years, critical information infrastructure (hereinafter "CII") entities were subject to hundreds or thousands of cyberattack attempts in 2021. However, the number of incidents registered by the NÚKIB in this category has decreased by about one quarter compared with the preceding year. **Yet the proportion of incidents resulting in limited service availability has risen to 70%** (Graph 19). Availability is one of the crucial elements for CII, and its disruption may have significant consequences (see the box below). Attackers are well aware of this, and ransomware gangs in particular rely on the high pressure to maintain or recover CII operation during their attacks, which increases the likelihood of the ransom being paid.

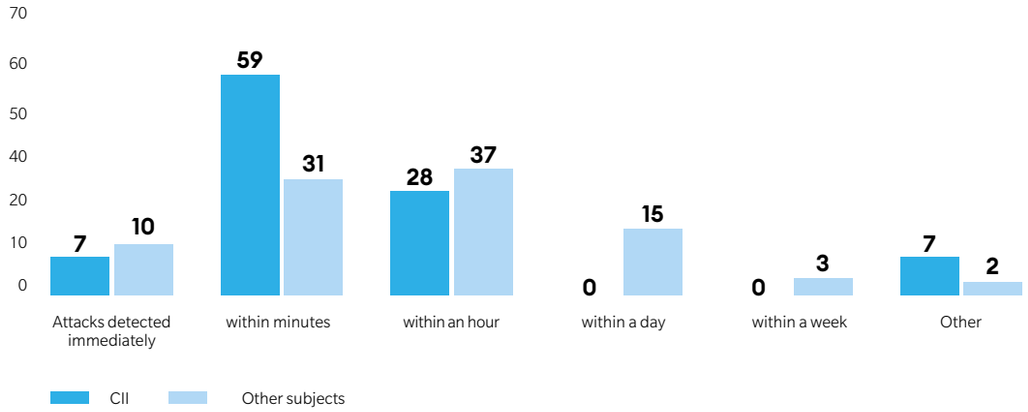
Graph 19: **Development of the share of incidents reported to the NÚKIB in the CII category resulting in limited availability between 2019 and 2021** (%)



Under Section 2(b) of the ACS, critical information infrastructure means an element or system of elements of critical infrastructure in the communication and information system sector within the field of cyber security. Pursuant to Section 2(g) of Act No 240/2000, on crisis management and on the amendment of certain other laws (Crisis Act), as amended, critical infrastructure is defined as an element or system of critical infrastructure elements whose compromise would have a significant impact on national security, on ensuring the basic living needs of the population, on people's health, and on the economy of the state. Typical critical infrastructure elements include power plants, dams, airports, telecommunication networks, strategic financial institutions, and state authorities. **Disrupting any of these elements could paralyse the provision of critical services (such as energy, heat, water, or pension payments) or, in extreme cases, cause physical harm (through cyber sabotage, for example).**

The high number of attacks directed at limiting availability likely (55%–70%) affected the speed of identifying the cyberattacks. While 92% of attacks on CII were detected within several hours, only 77% of attacks on other entities were identified within the same time. However, coping with the impacts of incidents was more challenging for CII entities. As many as 21% of CII entities needed weeks or even months to deal with the impacts of an incident (Graph 20), compared with an average of 17% in the case of other entities.

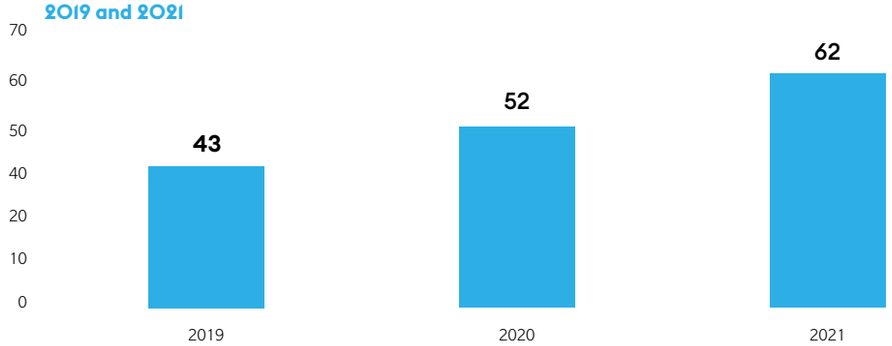
Graph 20: **Average time needed by respondents to identify a cyberattack in 2021** (%)



Public Sector: High Number of Incidents and Improved Funding

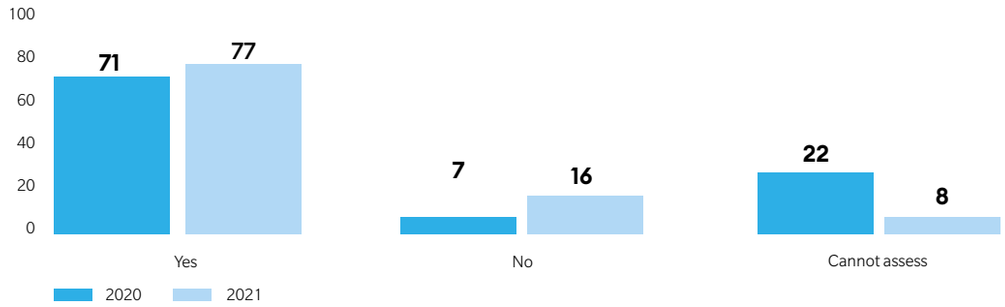
The public sector was one of the most affected in 2021, **accounting for nearly 40% of all cyber security incidents registered by the NÚKIB.** In addition, the number of incidents in this sector has been continuously growing (Graph 21). As in the preceding year, the most frequent recorded attack types included phishing, scam emails, and external network scanning. Institutions perceived ransomware, and attempts to exploit vulnerabilities in particular, as the most serious.

Graph 21: **Development in the number of public sector incidents registered by the NÚKIB between 2019 and 2021**



Despite the relatively high number of incidents, **more than three quarters of public sector entities perceive their cyber security as sufficient** (Graph 22). Up to 89% of respondents believe that their cyber security has improved. This might also be linked to the fact that the budgets allocated to cyber security have at least somewhat improved compared with 2020, which was affected by the pandemic crisis. While the budgets of nearly half the institutions decreased in 2020, the budgets of only 8% of the entities decreased in 2021. The budgets of two thirds of the entities remained the same, or even increased in the case of one fifth of the entities.

Graph 22: **Do you see the cyber security in your organisation as sufficient?** (% comparison between 2020 and 2021)



Financial Sector: Fairly adequate Security and Funding

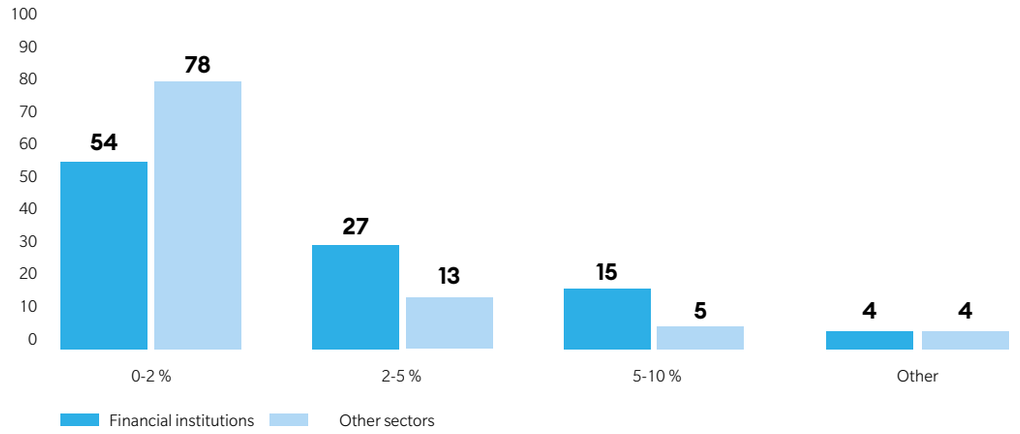
The Czech financial sector is probably one of the best-secured sectors, which is also indicated by the absence of more serious incidents in 2021. Despite a good level of security measures, the sector was not spared cyberattack attempts. **Up to 81% of financial institutions detected an attack attempt in 2021. The most frequent attack types targeting the financial sector included phishing, scam emails, and various types of malicious code.** Nearly one quarter of detected attacks resulted in at least one cyber incident. In 2021, attackers often aimed not only at financial institutions but also at their clients. **This was exemplified by the distinct increase in the number of vishing campaigns** (see the box).

Vishing attacks continue

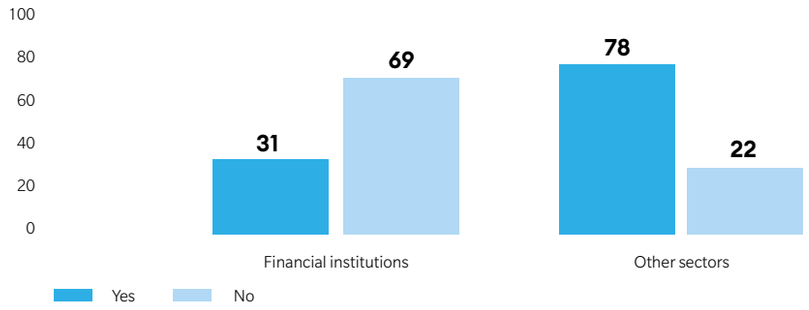
The trend of vishing attacks targeting clients of financial institutions continued in 2021. The NÚKIB, as well as the Czech National Bank (whose name was used in one of the vishing campaigns[x]), repeatedly warned against waves of scam phone calls. During their attacks, attackers usually exploit the names of legitimate institutions. Moreover, they are continuously improving their attacks, including by using fake articles, the Voice over Internet Protocol (VoIP) service to forge phone numbers, and encouraging users to install remote control software. Some banks have also noticed that attackers have started exploiting the increasing interest in investing in cryptocurrencies.[xii]

Many financial institutions are continuously seeking to improve their cyber security. This is evidenced, among other things, by the fact that 43% of them plan to increase their cyber-security budget for the coming year. **Compared with other sectors, financial institutions, on average, invested the highest percentage of their budgets in cyber security** (Graph 23). This is also due to their ability to afford the cyber security experts they need. More than two thirds of financial institutions have no problem offering adequate remuneration to such experts (Graph 24). Moreover, up to 90% of the respondents have the necessary funds for their regular training.

Graph 23: **Which percentage of the organisation's total budgets was allocated to cyber security costs in 2021?** (%)



Graph 24: **Comparison of the shares of entities in the financial sector and other sectors where salaries were the crucial factor discouraging applicants for jobs in cyber security in 2021** (%)



Industry and Energy: Ransomware as the Main Threat

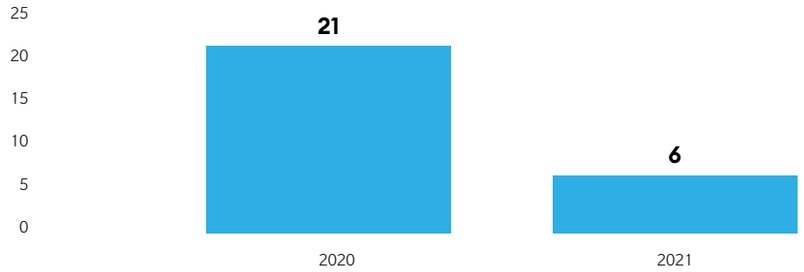
The international cyber security scene in the industry and energy sectors was mainly affected by massive ransomware attacks with unprecedented impacts in 2021. Attacks worth noting included, for example, the attacks on JBS Foods, the world's largest meat producer, Acer, an electronics manufacturer, and an attack on the American company Colonial Pipeline, which resulted in an outage of oil products on the East Coast of the USA (see the box below). **In the Czech Republic, there was one ransomware attack resulting in a production standstill at an energy-sector supplier in 2021.**

Attack on Colonial Pipeline

In 2021, the US energy sector saw one of the largest ransomware attacks so far. Colonial Pipeline, a company running the largest pipeline network in the USA, became a target of the ransomware group known as DarkSide. The attack affected the operational part of the network (accounting systems), but the company also had to switch off systems in the industrial network. As a result, the main source of oil product supplies for the entire eastern coast of the USA was shut off. The case highlighted the interconnectedness of business and industrial processes, and the significant dependency of industrial networks on operational networks.

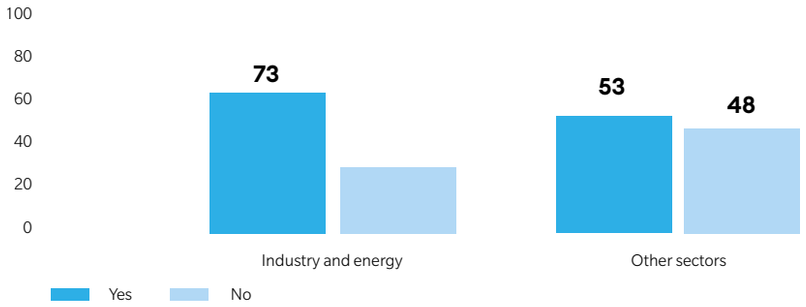
Ensuring the continuity of production and service provision is the priority goal of both the industry and energy sectors. Hence ransomware poses a significant threat to organisations in these sectors. This is also reflected in the fact that **it was considered one of the most serious threats even though only 6% of the respondents faced a ransomware attack or an attempt in 2021.**

Graph 25: **A year-on-year comparison of registered ransomware attacks or attempts in the industry and energy sectors** (%)



The significant emphasis on ensuring the continuity of operation and production in the industry and energy sectors is reflected in their high-level preparedness for a potential incident. A total of 73% of the surveyed companies from the industry and energy sectors have a cyber security incident crisis scenario as part of their crisis management procedures. Up to 97% of the respondents from the sectors in question create off-line backups of critical systems, and 78% of them test the backups regularly. Almost 80% of the entities have introduced Business Continuity Management (BCM) procedures. This means that the industry and energy sectors are well above average in the aforementioned attributes (see Graph 26, for example).

Graph 26: **If your organisation has established crisis management procedures, do the crisis scenarios include a cyber incident handling procedure?** (%)



Healthcare: A Slight Decrease in Ransomware Attacks and Continuously Insufficient Funding

The number of incidents in the healthcare sector registered by the NÚKIB increased by 34% year on year, with nearly half the incidents being assessed as significant or highly significant.[11] To some extent, the increase may be linked to the increase in the number of regulated entities in the healthcare sector obliged to report incidents (see the box below). **On the other hand, the number of registered ransomware attacks in healthcare has slightly decreased, which is in accordance with the data available to the NÚKIB.** This has also affected the perception of its severity, with ransomware no longer being considered the most serious threat. In 2021, healthcare entities perceived phishing, spear-phishing, and vulnerability exploitation attempts to be the most serious threats.

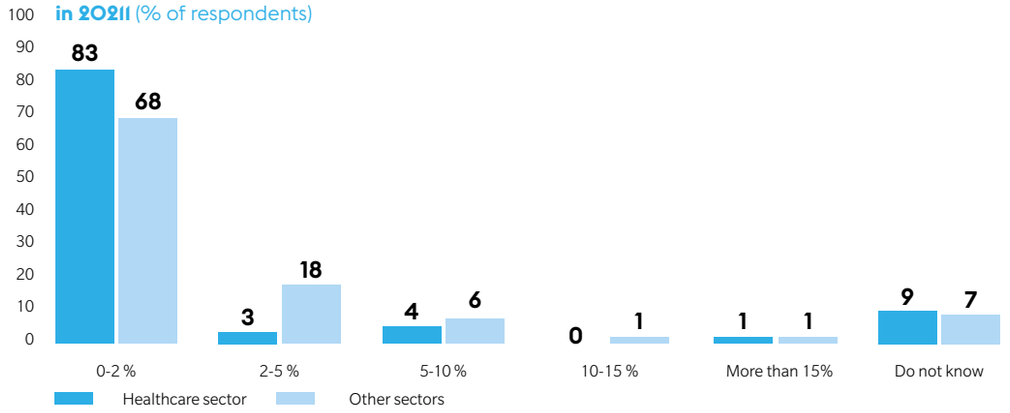
Amendment to the Decree on Operators of Essential Services in the Healthcare Sector

In reaction to the cyber incidents that healthcare facilities in the Czech Republic faced in 2020, the NÚKIB in cooperation with the Ministry of Health prepared an amendment to Decree No 437/2017, on the criteria for the determination of an operator of essential service, as amended, which became effective on 1 January 2021. The aim of the amendment was to change the criteria for the determination of essential healthcare services so that more hospitals would be identified as operators of essential service. Determination administrative proceedings were initiated with the relevant hospitals shortly after the amendment became effective. Thanks to the readiness on both sides, the proceedings were very quick and seamless. In 2021, 28 hospitals were identified as operators of essential service and the number of essential healthcare service operators thus rose to 44.

The full wording of Decree No 573/2020, amending Decree No 437/2017, on the criteria for the determination of an operator of essential service, is available at: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=39032

Although the funds allocated to cyber security increased in the case of more than one third of the entities compared with the preceding year, most of them they still ranged between 0% and 2% of the overall budget, which is far below the average of the remaining sectors (Graph 27). **At the same time, nearly 70% of the respondents considered the funds allocated to cyber security insufficient.** More than one third of the entities would increase their cyber security budget by more than 100%. Despite the somewhat unfavourable financial conditions, 88% of healthcare entities believe their cyber security has improved.

Grphf 27: **Share of overall budgets allocated to cyber security in healthcare and other sectors in 2021** (% of respondents)



[11] The severity of cyber incidents is defined in Decree No 82/2018 and the NÚKIB's internal methodology.

Education: Manyfold Growth in Cyber Incidents

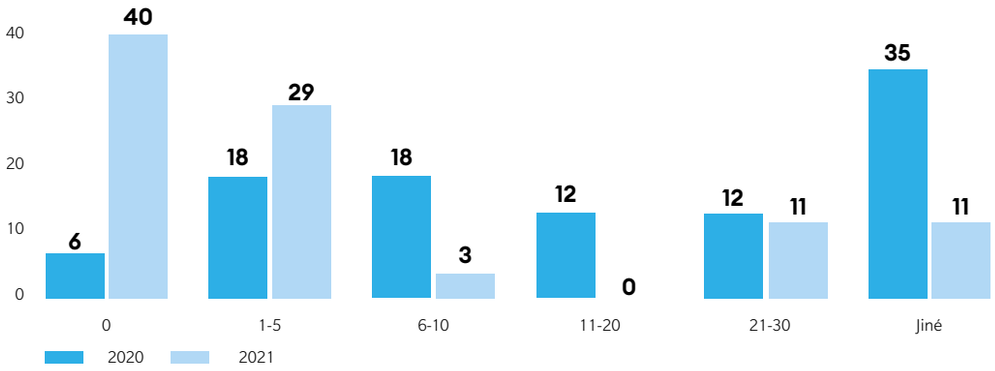
In 2021, the education sector saw a more than sixfold increase in the number of incidents registered by the NÚKIB. Although the number of regulated entities in education increased due to an amendment to Decree No 317/2014, on important information systems and their determination criteria (see the box), as amended, this change did not significantly affect the number of registered incidents. **The majority of incidents in the education sector were reported by non-regulated entities.**

On 1 January 2021, Decree No 360/2020, amending Decree No 317/2014, on important information systems and their determination criteria, as amended by Decree No 205/2016, became effective. Based on this Decree, information systems in the education sector may also be categorised as important information systems. In connection with this, the NÚKIB issued a supporting material entitled Important Information Systems in the Education Sector, which provides answers to the most frequently asked questions regarding the determination of these systems:

https://www.nukib.cz/download/publikace/podpurne_materialy/2021-02-22_VISskoly_ FAQ_v.0.1.pdf

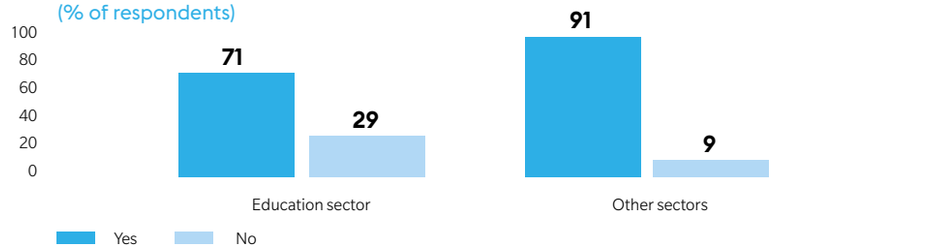
In spite of the high number of incidents registered by the NÚKIB, the number of attacks and attempts registered by entities in the education sector somewhat decreased (Graph 28). However, it cannot be ruled out (25%–50%) that the decrease is caused by the low capability of educational institutions to detect an attack or attackers' efforts to remain unnoticed. The latter scenario is particularly relevant in the case of higher education institutions, where **academic research is a very attractive target for statesponsored groups.**

Graph 28: **Year-on-year comparison of registered attacks or attempts in the education sector in 2021** (% of respomdents)



The education sector has become a target of numerous phishing campaigns in the last few years. In 2021, educational institutions considered phishing the most frequent and most severe types of attack, with **more than three quarters of the respondents registering a phishing attack or attempt**. The high rate of such attacks is increasing the need for education and growing awareness among employees of these institutions and other users in this sphere. Nevertheless, only 71% of entities in education provide user training, 15% less than in other sectors (Graph 29). Only one quarter of educational institutions allocate funds specifically to user training.

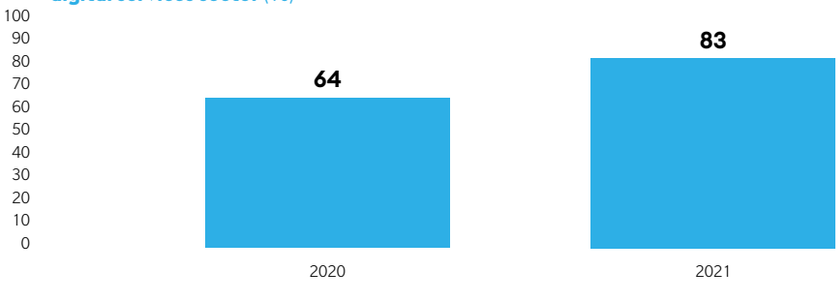
Graph 29: **Do you train users in cybersecurity and familiarise them with current cyber threats?** (% of respondents)



Digital Services: Increasing Numbers of Malicious Code Attacks and an Emphasis on Supplier Risk Management

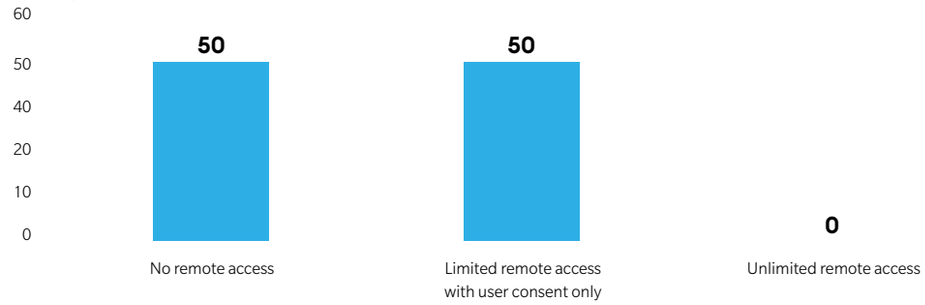
In 2021, Czech entities providing digital services (telecommunications, digital infrastructure, Internet services, etc.) most frequently faced external network scanning, phishing, and malicious code. **An attack or attempt using malicious code was registered by 83% of organisations, almost a fivefold increase compared with the preceding year** (Graph 30). Moreover, this type of attack accounted for more than 50% of the incidents registered by the NÚKIB in this sector. This is probably a key reason why an overwhelming majority of the entities considered malicious code the most serious type of attack.

Graph 30: **Year-on-year comparison of registered attacks or attempts using malicious code in the digital services sector** (%)



Institutions and organisations in the digital services sector are well aware of the necessity to secure the supply chain and therefore devote resources to supplier security risk management. All the respondents have set minimum security measures for contractual relationships, and some manage risks through technical or organisational measures. None of the respondents granted their suppliers remote access to their networks, while a half granted restricted access following the user's consent (Graph 31). The strong emphasis on risk management by entities providing digital services is likely (55%–70%) one of the reasons why 80% of them perceive the threat of a cyberattack through a service provider as low.

Graph 31: **What level of access to your networks do you grant your suppliers?** (% of subjects in the digital services sector)



Measures

Timeline of Measures and Alerts Issued by the NÚKIB in 2021

March

Reactive measure in connection with the Microsoft Exchange Server vulnerability
At the beginning of March, the NÚKIB warned about the active exploitation of severe vulnerabilities affecting Microsoft Exchange Server. Following this alert, the NÚKIB issued a reactive measure imposing an obligation to perform relevant security updates without delay on entities governed by the ACS, and to verify whether their systems have been compromised.
https://www.nukib.cz/download/uredni_deska/Opatreni_obecne_povahy_2021_03_11.pdf

April

Alert regarding the increased risk of cyberattacks against the Czech Republic
The following month, the NÚKIB issued an alert about the increased risk of cyberattacks against the Czech Republic in reaction to national and international affairs. It contained an analysis of the techniques most frequently used by attackers and the most frequently exploited vulnerabilities.
https://www.nukib.cz/cs/infoservis/aktuality/1703-hrozi-zvysene-riziko-kybernetickych-utoku-vuci-ceske-republice/

May

Alert regarding the Avaddon ransomware campaign
Another alert was motivated by an ongoing campaign by attackers operating the Avaddon ransomware who, among others, focused on Czech institutions and organisations. The use of this ransomware ceased at the beginning of June.
https://www.nukib.cz/cs/infoservis/hrozby/1717-upozorneni-na-probihajici-kampan-ransomwaru-avaddon/

August

Alert regarding active exploitation of the Microsoft Exchange Server – ProxyShell vulnerability
In August, the NÚKIB warned about a series of vulnerabilities affecting Microsoft Exchange Server. Although the vulnerabilities had been fixed by security updates released in the preceding months, they could still be exploited in combination with a ProxyShell attack.
https://www.nukib.cz/cs/infoservis/hrozby/1739-upozorneni-na-aktivni-zneuzivani-zranitelnosti-microsoft-exchange-server-proxyshell/

October

Protective measure in the form of a general measure to secure email boxes
For the first time ever, a protective measure was released to secure the communication of administrators and operators of information systems crucial to the functioning of the state and the safety of its citizens. The measure imposed an obligation to introduce a set of technical measures for obliged entities to better secure electronic mail. In addition to this measure, the NÚKIB also issued a detailed methodological guideline.
https://www.nukib.cz/download/uredni_deska/2021-10-08_OchranneOpatreni_final.pdf

November

Alert regarding a campaign exploiting an Exchange Server vulnerability
A new wave of exploitations of the Proxyshell vulnerability for the sophisticated delivery of phishing messages containing malware resulted in the issuance of a alert recommending that all Exchange Server administrators perform updates without delay.
https://www.nukib.cz/cs/infoservis/hrozby/1766-upozorneni-na-kampan-zneuzivajici-zranitelnosti-exchange-server/

December

Reactive measure in connection with the Log4Shell vulnerability
Shortly after the alert regarding the serious vulnerability in the Apache Log4j component, which affected a large number of widely used products and applications, the NÚKIB decided to issue a reactive measure containing obligatory tasks and a methodological guideline to secure systems.
https://www.nukib.cz/download/uredni_deska/2021-12-15_RO-NUKIB-Log4Shell.pdf

National Cyber Security Strategy: Action Plan and 5G Network Security

Action Plan for the National Cybersecurity Strategy of the Czech Republic from 2021 to 2025

The Government approved the **Action Plan** in July 2021. Although the NÚKIB spearheaded this project, it was created with significant contributions from all Czech public institutions with key roles in cyber security.

The Action Plan constitutes an implementation part of the already approved National Cyber Security Strategy of the Czech Republic. Both documents are closely interwoven and provide a clear idea of the Czech Republic's intentions in the area of ensuring cyber security for the following five years. The Action Plan sets out a total of 105 tasks for the period from 2021 to 2025, appoints the entities responsible for the implementation of each of them, and stipulates their implementation schedule. Some of the tasks are set as continuous (for example, in education or organisation of training), while others require more complex changes (such as preparing a draft of the National Coordinated Vulnerability Disclosure Policy). An evaluation of the Action Plan for 2021 is provided in Annex I to this Report.

The Action Plan is publicly available on the NÚKIB website at www.nukib.cz/cs/kybernetickabezpecnost/ strategie-akcni-plan/.

Addressing 5G Network Security

In 2021, the NÚKIB and other state institutions cooperated on developing security rules for 5G networks by creating proposals for introducing several EU 5G Toolbox measures into the Czech legal system. Besides the NÚKIB, which initiated and coordinated the activity, representatives of other state institutions responsible for the security of electronic communication networks and the protection of security interests of the Czech Republic participated in the preparation.
Based on the decision of the National Security Council and in cooperation with other state institutions, the NÚKIB prepared possible courses of action to ensure the cyber security of 5G networks. Once the National Security Council chose the most suitable option, the NÚKIB, together with other involved institutions, drew up a concept entitled **"Mechanism for the Assessment and Limitation of Risks Associated with 5G Network Suppliers"**, which will be further developed into the intended subjectmatter of the law.
Meetings of the working group on cyber security of the 5G Alliance, the platform for regular communication between the state and the telecommunications sector, were held throughout 2021. Within this group, sector representatives were regularly informed about the latest developments in 5G network security at national level.

Countering Hybrid Activities

The **National Strategy for Countering Hybrid Action**, the first of its kind in the Czech Republic, was drawn up in coordination with the Ministry of Defence and in cooperation with other institutions. It aims to address the changing security environment and to define the tools needed to protect the vital, strategic, and other significant interests of the Czech Republic from hostile hybrid actions. The Strategy defines goals in the following areas:

- **resilient society, state, and critical infrastructure;**
- **a systemic and holistic approach to security;**
- **adequate and timely reaction.**

The Strategy is available at https://mocr.army.cz/images/id_40001_50000/46088/N__rodn___strategie_pro___elen___hybridn__mu_p__soben__.pdf

Legislative Framework: An Increase in Obliged Entities and Changes in Cloud Computing

Identification and reassessment of critical information infrastructure, important information systems, and essential services

The NÚKIB has been identifying CIIs based on its mandate stipulated in the ACS and the Crisis Act[12] and in compliance with the Government Directive on Criteria for the Identification of CII Elements since 2015. The ACS obliges the NÚKIB to verify that the identification of CII elements is up-to-date every two years. A CII element is an information or communication system that meets the criteria stipulated in the above directive determining its importance for the preservation of vital functions of the state. The administrators of CII elements are both state and private entities. **In 2021, eight new CII administrators were identified, and the already identified CII elements were reviewed by 28 CII administrators.** Consequently, the NÚKIB currently registers 60 entities that administer 131 CII elements.
On 1 January, an amendment to Decree No 317/2014, on important information systems and their determination criteria, as amended, became effective. The decree introduces the so-called important information systems in state and regional establishments, which are listed in Section 2 paragraph 1 of the decree. The aforementioned section is under the so-called "split force" regime, meaning it will come into effect gradually, and new systems will be added every year until the decree reaches its final form in 2023. **A total of 90 public sector institutions and 196 important information systems were identified in 2021.**

Estimated increase in the number of important information systems due to the amendment to the Decree on Important Information Systems	
Period	Number of newly included systems
2022	610
2023	690
Total	690

The process of identifying operators of essential service was underway in 2021, mainly in the healthcare, energy, water management, and transport sectors. **In total, 70 entities were newly identified as operators of essential service, while decisions were made on non-identification in 51 administrative proceedings.** Hence, by the end of 2021, the total number of identified operators of essential service and essential service information system operators was 124 and 147, respectively.

Number of obliged entities by the end of 2021:

- administrators and operators of CII information and communication systems: **60 entities;**
- information and communication systems of the CII: **131 information and communication systems;**
- administrators and operators of important information systems: **162 entities;**
- important information systems: **372 information systems;**
- administrators and operators of essential service information systems: **124 entities;**
- essential service information systems: **147 information systems.**

[12] Act No 240/2000, on crisis management and amending certain other laws (Crisis Act), as amended, in compliance with Government Regulation No 432/2010, on the criteria for identifying a critical infrastructure element, as amended.

Legislative Changes in the Area of Cloud Computing and Compliance with Security Criteria Assessments

Since August 2020, the Ministry of the Interior has been assessing cloud computing providers and services. The NÚKIB is intensively engaged in this activity, assessing the fulfilment of obligatory security criteria for cloud computing providers who wish to provide public administration services. By the end of 2021, the NÚKIB had already issued 145 assessments in this area.

The year 2021 brought significant legislative changes linked to cloud computing issues:

- an amendment to Act on Public Administration Information Systems that modifies and specifies the assessment process for cloud computing providers and for individual cloud computing services where they are provided to public administration bodies;
- Decree No 315/2021, on security levels for the use of cloud computing by public authorities, defines the criteria for categorising information and communication systems of public administration bodies within security levels;
- Decree No 316/2021, on some requirements for incorporation into the cloud computing catalogue, further specifies the requirements that cloud computing providers and the services they offer must meet to be listed in the cloud computing catalogue.

In 2021, the NÚKIB assessed another four providers in relation to the requirements set out in Decree No 316/2021. No cloud computing was assessed in this regard in 2021 because the NÚKIB did not receive any application for cloud computing assessment in relation to the requirements stipulated in the decree in 2021. This is because the provider must be assessed first, and they can only apply for a cloud computing assessment afterwards.

NÚKIB Consultancy, Workshops, and Support Materials

A number of consultations regarding the implementation of the Act on Cyber Security were held in 2021. Besides individual consultations, there were also workshops on issues relating to the identification of important information systems, which were attended by 246 people from 68 state organisations. The NÚKIB continues to issue public support materials intended for both obliged entities pursuant to the ACS and the professional public. For example, the following materials were issued or updated in 2021:

- **guidelines for the determination of critical information infrastructure;**
- **requirements for contracts with suppliers;**
- **the operator of an information or communication system;**
- **guide to security level classification for cloud computing.**

In addition, the FAQ section of the NÚKIB's website was significantly updated, and now contains more information and answers to questions that the NÚKIB encounters: **https://www.nukib.cz/en/cybersecurity/regulation-and-audit/faq/ .**

The NÚKIB's Supervisory Activities in 2021

In terms of inspection and audit activities, in 2021 the NÚKIB was mainly occupied by mapping the state of cyber security at the most important healthcare facilities in the Czech Republic. **The number of inspections and audits** under the ACS or its Implementing Decree No 82/2018 on security measures, cyber security incidents, reactive measures, cyber security reporting requirements, and data disposal (the Cyber Security Decree), as amended (hereinafter the "CSD") **increased from 8 to 22 in 2021**. Inspections or audits at obliged entities and persons by Section 3 of the ACS verify that the obligations resulting from the ACS and CSD are being met. Each inspection or audit generally verifies approximately 150 checkpoints. **In addition to the healthcare sector, the NÚKIB also focused on other entities in 2021, such as evaluating the system that ensures the processing and presentation of election results at the Czech Statistical Office.** The NÚKIB performed a comprehensive audit, including a mock phishing campaign, vulnerability scanning, implementation of internal and external penetration tests, and stress tests. The comprehensive audit also involved table-top training, through which the Czech Statistical Office could test its preparedness for crisis situations relating to the processing and presentation of election results, including in the media. Last but not least, an audit of the system's compliance with the requirements of the CSD was performed.

Cooperation between the NÚKIB and Other Supervisory Bodies on Inspections in 2021

In 2021, the NÚKIB continued to develop cooperation in inspection activities with other regulatory bodies. Namely, it signed a memorandum on cooperation with the Civil Aviation Authority, which also relates to cooperation in other areas than inspections. Practical cooperation in the area of inspections was developed with the Czech National Bank during a joint inspection, in which NÚKIB staff participated in the control group as an invited party. An important goal of the cooperation between the NÚKIB and authorities cooperating in the area of inspections is an effort to minimise the burden placed on obliged bodies and persons.

The inspection and auditing activities most often uncovered deficiencies in the following areas:

- **the set cyber security system does not cover the requirements of all interested parties;**
- **entities inadequately manage cyber security assets and risks;**
- **security policies and security documentation are often not put into practice or are not up-todate;**
- **entities inadequately manage supplier risks;**
- **obsolete hardware and software that the manufacturer no longer supports are used; the associated risks are not managed;**
- **insufficient numbers of cyber security experts;**
- **inappropriate network segmentation;**
- **insufficient internal network monitoring;**
- **log records are kept for too short a period;**
- **the activity continuity system is not functional.**

Cyber Security Exercises: Gaining New Experience on National and International Level

Although activities held in 2021 continued to be affected by the pandemic, it became possible to once again hold physical training events and other activities. The NÚKIB therefore focused on preparing new exercises and organising training events that could not be held in 2020.

National exercises	International exercises
9	**5**

In this respect, Health Czech, the first ever cyber security exercise in the healthcare industry, was a significant achievement. The trainees were representatives from 16 hospitals, whose teams included IT workers, (cyber) security experts, lawyers, press secretaries, and curative and preventive healthcare staff. The objective of the training was to get all these various professions involved and thereby encourage their mutual cooperation and a common view of and approach to cyber security. The knowledge gained during Health Czech will also be used in another training intended for the healthcare sector to be held in 2022.

Outlook for the Future Direction of Cybersecurity Exercises:

Considering the increasing number of regulated entities and the demand for training, sector-focused training for larger numbers of relevant participants appears as the best approach. Future trainings could also employ the **"train-the-trainer"** concept, whereby experts from the NÚKIB can share their know-how and best practices with experts from individual entities to enable them to create training tailored to the needs of their organisations. The NÚKIB will therefore, in the following period and as far as available capacities allow, continue with the consultations on creating trainings requested last year.

Several cyber security exercises with international participation were also held in 2021. The first of them was the largest cyber security exercise in the world, Locked Shields 2021. For the first time, this exercise was held remotely, and most organisers (including representatives of the NÚKIB) and participants had to handle the tasks online using collaboration and communication platforms. The remote form brought about much valuable experience and tested participants´ ability to cooperate on the national and international level. The training focused on the protection of both civilian and military IT systems, and critical infrastructure systems. It comprised a technical part, as well as legal, communication and analytical aspects. **The Czech national team, consisting NÚKIB representatives, other national organisations, the private sector, and academics ranked 3rd out of 22 teams, continuing the successful trend from preceding years.**

Czech Republic's ranking in Locked Shields exercises over the last five years				
2017	2018	2019	2020	2021
1st	3rd	2nd	cancelled	3rd

Other international trainings held last year were the Cyber Coalition and CRISIS-X. Cyber Coalition is an international cyber security exercise organised by the North Atlantic Treaty Organization. On the national level, the NÚKIB coordinates the civilian part, and the Cyber and Information Warfare Command coordinates the military part. The name of this event emphasises its goal: to encourage a stronger union and cooperation within. It is done by constructing scenarios focused on addressing technical challenges, encouraging cooperation among the individual countries, and creating a common awareness of the situation. CRISIS-X was the first joint training between the NÚKIB and the Israel National Cyber Directorate (INCD), during which teams from various authorities tested mutual communication as well as their ability to handle incidents on the national level.

Important Findings from Exercises in Preceding Years:

- **methodical and background materials created by the NÚKIB following new or amended legal standards and issued measures are beneficial and provide the relevant staff of numerous entities with useful support in implementing the above-mentioned;**
- **the lack of funds and human resources is a common problem in cyber security. Nevertheless, sufficient funding still need not ensure adequately qualified staff, as can be seen in the Czech Republic, which is experiencing staff shortages in this field;**
- **entities are increasingly aware that training ordinary staff is crucial in ensuring cyber security.**

Awareness-Raising and Education in the Czech Republic: A Focus on Target Groups as well as the Broader Public

Education and awareness-raising in cyber security remain important society-wide topics. Due to the pandemic, there was a growing need to address the security aspects associated with the increased engagement of digital technologies in all spheres of life. This also entailed increased demands on the preparedness of Czech citizens in terms of the secure use of digital technologies and movement in the online world across all social groups, whether performing employment-related activities or studying, for example.
As in preceding years, the awareness of staff at public administration and obliged entities of cyber security risks was targeted through the course in cyber security basics called **Dávej kyber!** (Get Cyber Skilled!) and the course **Šéfuj kyber!** (Manage Cyberspace!) intended for cyber security experts. More attention was paid to education and awareness-raising in the healthcare sector last year. In the spring of 2021, the NÚKIB created and launched an online course in cyber security basics for healthcare staff called **Kyber nemocnice!** (Cyber Hospital!). Based on feedback from hospitals, the NÚKIB also responded to the need to educate healthcare staff that only use digital devices and information technologies on the basic user level by creating the course **Startuj kyber!** (Start in Cyber Security!). The course on the foundations of safe behaviour on the Internet called **Bezpečně v kyber!** (Stay Safe in Cyberspace!), primarily intended for education and prevention staff, teachers and headmasters, was newly opened to the general public as well.

Number of Users Who Have Completed NÚKIB Courses	
Dávej kyber!	26,146
Šéfuj kyber!	441
Kyber nemocnice!	4,407
Bezpečně v kyber!	2,841

Great efforts were made in 2021 to raise awareness and educate children and students in kindergartens, primary schools, secondary schools, and higher education. The following activities and projects were carried out last year:

- The NÚKIB released a new **directory of educational materials for schools** with materials suitable for promoting cyber security awareness within teaching in kindergartens, primary schools, and secondary schools.
- The NÚKIB participated in creating the book **"Kyberpohádky"** (Cyber Fairy Tales), exploring the various threats children can encounter in cyberspace. The project author is Centrum kybernetické bezpečnosti, z. ú.
- In cooperation with ENISA, the NÚKIB created a special **series of educational posts** that were shared on the Instagram account **@petr.vytrzny** throughout October – European Cyber Security Month. There were more than 3,500 reactions to the posts.
- With the help of Zásilkovna, Safer Internet Centre distributed **Safe Internet Noticeboards** to all primary schools in the Czech Republic. This distribution was supported by the NÚKIB and the Ministry of Education, Youth, and Sports.
- **Ámos Vision interactive panels**, in which pupils can try out the educational activities related to cyber security prepared by the NÚKIB, were placed in 200 schools.
- The educational activities **Digitální stopa: Příběh Báry** (Digital Footprint: Bára's Story) and **Digitální stopa: Příběh Svůďáka** (Digital Footprint: Tom's Story) were updated and expanded to include pressing cyber security topics. The latter of the two courses was reworked as a chatbot in cooperation with the EduKids initiative. More than 3,900 users used it in the very first month of its release.

- In cooperation with the Smíchov Secondary School of Industry and several popular influencers, the NÚKIB created an educational **video course** entitled **Jsem netvor, tvor, který žije na netu!** (I'm a beast, a creature living on the Internet!) for students from primary and secondary schools, familiarising them with the dangers of digital technologies.
- The NÚKIB created a video course entitled **Jsem netvor na střední** (I'm a secondary school beast) for secondary-school non-IT study programmes to help spread cyber security knowledge.
- Nearly 400 schools and 5,500 students from around the country competed in the **6th National Cyber Security Competition.**
- The first fair trade of study programs for primary and secondary school students called Studuj kyber! took place as part of the **CyberCon conference**. The trade fair aimed at presenting schools and study programmes concentrating on cyber and information security and information technologies.
- The NÚKIB continued to develop its cooperation with higher education facilities preparing cyber security experts. The NÚKIB signed a Memorandum of Cooperation with the University of Defence for the education of cyber security specialists.

Furthermore, many awareness-raising and educational activities for the broader public were held in 2021:

- One significant event was the **7th European Finals of the European Cyber Security Challenge** in Prague, organised by the Czech branch of AFCEA in cooperation with ENISA. The finals were attended by 163 competitors from 19 countries, and included various events, bilateral and multilateral discussions, and a specialist conference on cyber security and artificial intelligence.
- The course **"Příběhy sociálního inženýrství"** (Tales of Social Engineering) focusing on scam communication, social engineering techniques, and ways of preventing them, was created under the auspices of the Masaryk University.
- **"Kyberkampaň"** (Cyber Campaign), an awareness-raising campaign focusing on phishing (vishing), created in cooperation with the Police of the Czech Republic, the Czech Banking Association, and ESET, was run last year. It included "Kybertest" (A Cybertest), an interactive training tool for training in how to detect scam communication.
- Another successful project was a **cyber security course for senior citizens**, implemented thanks to joint efforts of the cyberteam and the University of the Third Age of Masaryk University.
- Courses created by private companies were also held last year. Namely, **Sherlock senior** by Seznam.cz focusing on media education for the elderly, and **Digitální Odysea** (Digital Odyssey) by Vodafone, providing basic information about the use of smartphones and tablets in an effort to help the elderly adapt to modern society, in which more and more services are digitalised.

2021 CyberCon Conference[xii]

The NÚKIB held its 7th CyberCon Brno conference in September 2021, with the main objective to provide space to bring the public, academic and private sectors together in the field of cyber security. During the three-day conference programme, more than 300 visitors, both professionals and the general public, could hear various talks reflecting the technical, legal, and political aspects of cyber security presented by 37 speakers from the Czech Republic and abroad. The 7th CyberCon differed in many aspects from the ones in previous years. The biggest change was the expansion of the conference to include an international day held in English, with debates on amendments to the NIS Directive, the Cyber law toolkit, and quantum computing. Moreover, the "Protecting the Healthcare Sector from Cyber Harm" project was commenced at CyberCon. The conference was accompanied by various programmes, for example the educational opportunities trade fair Studuj kyber! (Study Cyber), a technical workshop, and a demonstration of table-top cyber security training.

International Cooperation: Active Involvement of the Czech Republic in Europe and Beyond

The development of Czech regulatory and coordinating tools largely depends on the development of the situation abroad and the decisions adopted on European and international levels. The NÚKIB, together with the Ministry of Foreign Affairs, the Ministry of Defence and other partners, represents Czech cyber security interests in international organisations and integration groups, especially in the EU, the UN, NATO, the OECD, the OSCE, and the ITU.[13] In 2021, Czech representatives mainly focused on negotiations regarding an **amendment to the NIS Directive, sounding interviews about a potential review of the applied measures**[14] **from the Cyber Diplomacy Toolbox**,[15] and initial negotiations concerning **the Joint Cyber Unit (JCU)** initiative. Meetings of the UN Open-Ended Working Group (OEWG) on the security of information and communication technologies, in which the NÚKIB and the Ministry of Foreign Affairs actively participate, were held last year. In 2021, the OEWG member states succeeded in establishing agreement and adopted the Final Factual Report containing recommendations regarding current and emerging cyber threats, international law, and trust- and capacity-building measures.

Prague 5G Security Conference a Prague Proposals

The NÚKIB, in cooperation with the Ministry of Foreign Affairs and under the auspices of the Office of the Government, held **the 3rd Prague 5G Security Conference** at the turn of November and December 2021. This conference, which was held in a hybrid form due to anti-pandemic measures, concentrated on issues associated with the security of 5G networks and Emerging and Disruptive Technologies (EDTs). Nearly seventy speakers from Europe and around the world (Israel, Korea, Japan, Australia, the USA, Canada and India, for instance) spoke at the conference. Representatives of the public, academic, non-profit and private sectors were also present at the conference. The two-day conference was divided into several thematic panels attended online by hundreds of international listeners.

At the end of the conference, the **"Prague Proposals on Cyber Security of Emerging and Disruptive Technologies"** regarding the cyber security of emerging disruptive technologies were presented. In them, the participating countries agreed on potential principles of future approaches to EDTs. Among other things, the document mentions the importance of taking into account both technical and nontechnical risks, supply chain security, transparency, credibility, and the diversification of democratic and ethical values in the development of new technologies. The outcomes of the 3rd conference also include the second Prague Proposals on the diversity of telecommunications suppliers **("Prague Proposals on Telecommunications Supplier Diversity").**

Newly presented Prague Proposals:

- **Prague Proposals on Cyber Security of Emerging and Disruptive Technologies**
  https://www.nukib.cz/download/Prague_Proposals_on_Cyber_Security_of_EDTs.pdf
- **Prague Proposals on Telecommunications Supplier Diversity**
  https://www.nukib.cz/download/Prague_Proposals_on_Telecommunications_Supplier_Diversity.pdf

[13] Ministry of Industry and Trade, Czech Telecommunication Office, and others.
[14] A set of tools for a joint diplomatic reaction by the EU to malicious cyber activities.
[15] The European Commission's initiative seeking to enhance and encourage cooperation between EU bodies, institutions, and other subjects and Member State bodies in cases where various cyber communities should closely cooperate to combat serious cross-border cyber incidents or threats.

Amendment to the NIS Directive and preparations for the Czech presidency of the European Council

In 2021, the Czech Republic participated in implementing specific initiatives of the EU Cybersecurity Strategy. This strategy and the amendment to the NIS Directive represent key documents anchoring the EU's political and legislative orientation with respect to cyber security.

Amendment to the NIS Directive

The draft amendment to the NIS Directive should significantly expand the sectors of obliged entities and unify the methods for their determination. Moreover, it should stipulate coordinated vulnerability disclosing, unify the methods of determination of obliged entities, and stipulate new incident reporting obligations to achieve greater harmonisation of the Member States' legislations and approaches in the area cyber security.
At the end of 2021, the European Council adopted a general approach (i.e. a shared position of the EU Member States), while the successful completion of negotiations on the final draft remains the priority for 2022.

In 2021, the NÚKIB started full preparations for the second Czech presidency of the European Council, which will see the Czech Republic take over from France in July 2022. Czech representatives participated in preparatory and coordinating meetings throughout 2021, such negotiations being crucial for the successful organisation and actual course of the presidency. The negotiations were held at national level, with EU institutions and, last but not least, with France and Sweden, with whom the Czech Republic forms a presidency 'trio'.

Cyber Security Trends and Outlook for the Czech Republic in 2022 and 2023

1. Ransomware
The use of extortion malware will almost certainly (90%–100%) remain one of the most significant cyber threats in the coming two years. The rising trend of RaaS and multiple extortion will almost certainly (90%–100%) continue in the next two years. With the onset of the now dominant RaaS model and the gradual decline of the COVID-19 pandemic, we could see a moderate decrease in ransomware attacks on the healthcare sector. Instead, highly sophisticated attacks on large and lucrative economic entities will occur. This trend will be highly likely (75%–85%) to continue in the coming period. Moreover, further development and innovations of the RaaS model are likely (55%–70%).

2. Vulnerabilities
The trend of the widespread exploitation of newly published vulnerabilities will be highly likely (75%–80%) to continue in the coming years. The rate at which attackers add new vulnerabilities to their tools has been increasing. In the case of Log4Shell, attackers started exploiting the vulnerability for their attacks within the first 24 hours of its publishing It is highly likely (75%–85%) that vulnerabilities will be exploited by both state actors and cybercriminal groups, particularly ransomware gangs. This trend is likely (55%–70%) to affect Czech institutions and organisations in the coming years and, consequently, the demands placed on effective management of vulnerabilities will increase.

3. Phishing, spear-phishing, and scam emails
It is almost certain (90%–100%) that the Czech Republic will continue to face phishing and spearphishing campaigns. These methods are still some of the most effective ways to get into a victim's system and hence are frequently used by malicious actors. It is highly likely (75%–85%) that they will become more and more sophisticated. The use of coronavirus--related topics is likely (50%–70%) to decrease thanks to the gradual decline of the pandemic. In the preceding period, vishing campaigns also occurred in the Czech Republic, and it is highly likely (75%–85%) that this type of attack will become more frequent in the next period.

4. Supply chain attacks
Information technology supply chains are getting more and more complex. This trend will almost certainly (90%–100%) continue. For attackers, these complex structures open up a way, used by both state actors and cybercriminal actors with increasing frequency, to potentially compromise a large number of victims. Therefore, supply chain attacks as a global trend are highly likely (75%–85%) to strengthen. It is likely (50%–70%) that their broad impacts may also affect entities in the Czech Republic.

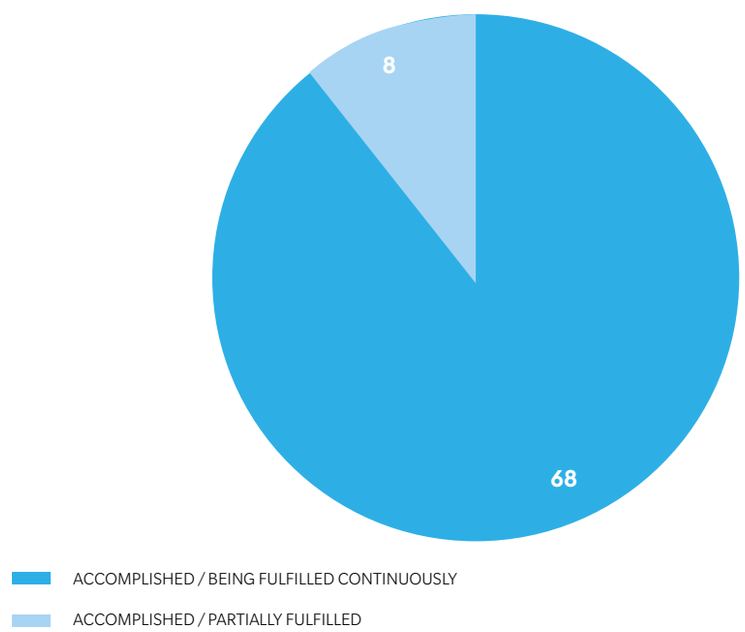
5. Cyberattacks against strategic state institutions
The state sector, including its strategic institutions, has long been a frequent target of cybercriminals and state actors. Since some state-endorsed actors may be especially interested in targeting Czech institutions due to the Czech Republic's geopolitical attitudes on some foreign policy and security topics, the likelihood of attacks may be affected by developments on the international scene. In addition, there is a realistic possibility (25%–50%) that some central public administration bodies have been long-term targets of persistent attackers trying to compromise them. The NÚKIB estimates that serious 48 cyberattacks against strategic state institutions is highly likely (75%–85%) to occur in the Czech Republic in the coming period.

Annex: Meeting the goals of the Action Plan for the National Cybersecurity Strategy of the Czech Republic from 2021 to 2025

In 2021, the Action Plan was evaluated for the very first time. The NÚKIB coordinates the evaluation of the Action Plan and also takes part in in fulfilling 101 tasks of the total of 105 tasks as an administrator or in cooperation with other entities. **The evaluation for 2021 addressed 76 tasks, 71 of which will be completed in a course of several years. Nearly 90% of the evaluated tasks have been accomplished or are being continuously fulfilled; 8 have been fulfilled only partially; and none of the tasks has been evaluated as not fulfilled at all** (Graph 32). An example of an accomplished task with a deadline in 2021 is the completion of an analysis of legal options for the rapid flexible purchase of technology and software for the deployment of countermeasures during crisis periods. The NÚKIB created a comprehensive internal summary with comments and consultations from the Ministry of the Interior and the Ministry of Regional Development. The document shows that the Czech legal system already allows for a flexible response to the specifics of individual situations and consideration of potential time constraints or the need to protect the state's security interests when selecting a public procurement supplier. Hence, no amendments to the legislation are required.

The COVID-19 pandemic-related measures continued to affect the fulfilment of many tasks. The measures largely limited cooperation in person, an essential precondition for the fulfilment of many tasks. One such example is the task to form a coherent approach within the Czech Republic to interpret existing international legislation on cyber security and defence. In-person meetings of the working group in charge of creating this national approach were not possible until the autumn of 2021 due to the pandemic measures. Consequently, a coherent national approach has not been formulated. Nevertheless, the actors managed to adapt to the anti-pandemic measures in many cases, and the tasks were effectively accomplished remotely (one example being the Locked Shields 2021 training). Efforts to finish both the tasks that have yet to be fully completed and multi-year tasks will continue in 2022 so that all tasks are fully implemented in a timely manner.

Graph 32: **Evaluation of the tasks from the 2021 Action Plan**



Sources

i **Lupa.cz. 2021. IT systémy Prahy a dalších státních úřadů byly napadeny kybernetickým útokem.** https://www.lupa.cz/aktuality/it-systemy-prahy-byly-napadeny-kybernetickym-utokem-servery-jsou-odstaveny/

ii **NÚKIB. 2022. Měsíc od vydání reaktivního opatření ke zranitelnosti Log4Shell: NÚKIB plošné zneužívaní v ČR neeviduje, přesto obezřetnost zůstává na místě.** https://www.nukib.cz/cs/infoservis/aktuality/1794-mesic-odvydani-reaktivniho-opatreni-ke-zranitelnosti-log4shell-nukib-plosne-zneuzivani-v-cr-neeviduje-prestoobezretnost-zustava-na-miste/

iii **The MITRE Corporation. 2021. Exploit Public-Facing Application**. https://attack.mitre.org/techniques/T1190/

iv **CrowdStrike. 2021. Ransomware as a Service (RaaS) explained.** https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

v **iROZHLAS. 2021. Olomoucký magistrát čelí několik týdnů hackerským útokům. Odmítá zaplatit výkupné.** https://www.irozhlas.cz/zpravy-domov/olomouc-magistrat-hackersky-utok-hackeri-ransomware-avaddon_ 2105221133_ako

vi **NÚKIB. Zpráva o stavu kybernetické bezpečnosti ČR za rok 2020.** https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf; **NÚKIB. Zpráva o stavu kybernetické bezpečnosti ČR za rok 2019.** https://www.nukib.cz/download/publikace/zpravy_o_stavu/NUKIB_ZSKB_2019.pdf

vii **Accenture. 2020. 2020 Cyber Threatscape Report.** https://www.accenture.com/_acnmedia/PDF-136/Accenture-2020-Cyber-Threatscape-Full-Report.pdf

viii **Securelist. 2021. APT annual review 2021.** https://securelist.com/apt-annual-review-2021/105127/

ix **Policie České republiky. 2022. Vývoj registrované kriminality v roce 2021.** https://www.policie.cz/clanek/vyvojregistrovane-kriminality-v-roce-2021.aspx

x **Česká národní banka. 2021. Vishing: Upozorňujeme na telefonáty zneužívající jméno ČNB.** https://www.cnb.cz/cs/dohled-financni-trh/ochrana-spotrebitele/upozorneni/Vishing-Upozornujeme-natelefonaty- zneuzivajici-jmeno-CNB/

xi **Moniová, Eva. 2021. Spořitelna varuje před dalším útokem. Lidé naživo sledují, jak jsou okrádáni.** https://www.seznamzpravy.cz/clanek/sporitelna-varuje-pred-dalsim-utokem-nachytaly-se-uz-desitky-lidi-174563

xii **For more information about the conference, please visit** https://www.cybercon.cz/eng/

ABOUT NÚKIB

The National Cyber and Information Security Agency (NÚKIB) is the central administrative body for cyber security, including the protection of classified information in information and communication systems as well as cryptographic protection. It is also responsible for the implementation of the regulated public service of the global navigation satellite system under the Galileo programme. It was established on 1 August 2017 on the basis of Act No 205/2017, amending Act No 181/2014, on cybersecurity and on amendments to related laws (Act on Cyber Security).

The NÚKIB currently helps ensure the cyber security of the Czech Republic and its citizens by:

- **providing timely, clear, and relevant information to critical information infrastructure entities, essential service providers, and public administration bodies;**
- **ensuring the security of classified information in information and communication systems including cryptographic protection;**
- **preparing national security standards, laws, and cyber security standards;**
- **providing technical support and other services, such as security verification using penetration testing techniques and providing vulnerability scans;**
- **providing a flexible response to cyber incidents using expertise and access to information for efficient incident handling;**
- **organising training and cyber exercises at both the national and international level;**
- **analysing trends in cyber security;**
- **providing methodological support, education, and raising awareness in cyber security -related topics;**
- **performing research and development in cyber security;**
- **performing cyber security risk assessments and adopting relevant remedial and preventive measures;**
- **checking compliance with requirements of the Act on Cyber Security at regulated bodies;**
- **representing the Czech Republic in international organisations active in the field of cyber security;**
- **cooperating with public, private, and academic sectors at both the national and international level.**

For more information about the NÚKIB, please visit our website at www.nukib.cz or follow the news in the field of cyber security in the Czech Republic on Facebook, Instagram, and Twitter.

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost