

**2020 REPORT
ON CYBER SECURITY
IN THE CZECH REPUBLIC**



FOREWORD BY THE DIRECTOR OF THE NÚKIB

Dear reader,

You are now presented with the 2020 Report on Cyber Security. It is needless to point out the many twists and turns the Czech Republic and the whole world went through that year. Yet I would still like to mention what the global pandemic has meant for cyber security.

Last year showed us all that the limits of what can be moved to cyberspace are far beyond what we previously imagined. Moreover, the transition has revealed how much we depend on information and communication technologies.

IT and cyber security experts have been drawing attention to this dependency for many years. It was not until last year, though, as the Internet became the only place where many people could work, close deals, hold talks, and keep in touch with loved ones, that we realised how overwhelming this reliance truly was.

Let us see this situation as an opportunity. The virus has helped us do what we had not been able to do ourselves: it persuaded the majority of society that cyber security, and the principles of proper conduct in cyberspace per se, are of concern to all of us.

The following texts and statistics indicate that cyberspace is not a safe place. No one can be unaware of the ransomware attacks that paralysed, among others, the University Hospital Brno during the onset of the pandemic, causing hundreds of millions of crowns of damage. Our statistics also show that the number of attacks has been growing, and more and more institutions – take local authorities as an example – have been falling victim to such attacks.

The National Cyber and Information Security Agency (hereinafter the 'NÚKIB') worked to give all possible assistance to the affected entities and protect others the attacks could also impact. Let me mention, inter alia, a reactive measure for selected healthcare entities followed by a warning issued for the same group of recipients. We also prepared many supporting materials that anyone may use free of charge to secure their systems.

We drafted changes in legislation, effective since January this year, especially for the healthcare sector. As a consequence, significantly more hospitals must meet

considerably stricter security requirements. At the same time, they have the opportunity to use broader services ranging from vulnerability scanning to penetration testing and other activities we offer regulated entities free of charge.

Furthermore, we have introduced several training courses for both the public and employees of essential institutions. People are the weakest link in cyber security, and they need to be aware of the risks looming in cyberspace.

Other unequivocal successes include the approval of two documents critical for developing the cyber security of the Czech Republic and the NÚKIB itself. Had it not been for them and the related collaboration, this 2020 Report on Cyber Security would not have seen the light of day. Nor, most importantly, could cyber security in the Czech Republic have been assured.

The first document is the National Cyber Security Strategy, which establishes the direction of activities for the agency and all subjects involved in cyber security assurance in the Czech Republic for the following five years. The other crucial document is the NÚKIB Development Concept, which sets out how the institution will develop going forward, the capacities we would like to have in the future and, last but not least, how much it will all cost. I am very pleased that the work on this document has been completed. The NÚKIB is still a new institution, and so a clear definition of its future development is vital.

Regarding the international scene, I would like to emphasise the 2nd Prague 5G Security Conference held under the auspices of the Czech Prime Minister and attended by many important foreign guests.

The developments last year showed us how dangerous cyberspace can be yet how important it is to all of us. I would like to thank all the 222 entities in various fields that filled in our questionnaires and thereby participated in preparing this 2020 Report on Cyber Security. I firmly believe that the Report will raise cyber security awareness and improve safety for everybody.

Ing. Karel Řehka

SUMMARY OF THE 2020 REPORT ON CYBER SECURITY IN THE CZECH REPUBLIC

The year 2020 was marked by an increase in cyber-attacks against Czech institutions, organisations, and companies across all sectors. Compared to 217 incidents in 2019, a total of 468 incidents were reported to the NÚKIB in 2020. Nearly one-third of the incidents handled were reported by non-regulated entities. This increase was very likely caused by both a higher number of cyberattacks and greater awareness of the existence and activities of the NÚKIB. The severity of the incidents has also increased, which is evident from the attacks against the University Hospital Brno and the Psychiatric Hospital in Kosmonosy. The most frequent types of attack in 2020 included **spam, phishing, and scanning**.

The most serious cyber threats in the Czech Republic have long included cybercrime. In 2020, this was most visible with **ransomware attacks affecting the Czech healthcare sector**. The increase in attacks against hospitals can largely be attributed to the ongoing pandemic as well as cybercrime groups concentrating on specific institutions where they see a higher chance that the ransom will be paid. Yet three-quarters of healthcare facilities consider the funds allocated to ensuring cyber security insufficient.

In 2020, the NÚKIB, in cooperation with the Office of the Government and the Ministry of Foreign Affairs, organised the second two-day Prague 5G Security Conference, the world's premier forum for discussion of the risks associated with the building of 5G infrastructure. As last year, the conference was held under the auspices of Andrej Babiš, the Prime Minister of the Czech Republic. Despite the fact that the conference was virtual for the first time due to the COVID-19 situation, more than 50 speakers from Europe, the USA, South Korea, Israel, Australia, India, and other countries spoke at it. The main outcome of this second conference was the presentation and launching of the so-called **Prague 5G Security Repository**, a virtual library

intended for sharing legislative, strategic, and other 5G network security tools the countries adopted over the past year.

In 2020, the NÚKIB continued the training of public administration staff and trained more than 18,209 civil servants, 214 employees of the Armed Forces of the Czech Republic, and 2,000 employees of Bulovka Hospital in the 'Dávej kyber!' [Get Cyber Skilled!] e-learning course. Another **1,690 prevention officers** were trained in the professional 'Bezpečně v kyber' [Stay Safe in Cyberspace] course, which presents school environment situations to staff.

Many organisations questioned through the survey said they faced a lack of experts and insufficient cyber security budgets in 2020. The situation was more pronounced in the public sector than in private undertakings. Almost none of the respondents had all cyber security posts occupied. More than half the organisations considered insufficient salaries to be the main factor.

In response to events during the pandemic, the NÚKIB issued several recommendations, warnings, and reactive measures. These included, for example, warnings about the risks associated with online conference services, **Safe Remote Working** recommendations, the **Secure Videoconferencing** manual, and the **Minimum Safety Standard** document for securing smaller organisations prepared in cooperation with NAKIT.

Despite the pandemic measures, Cyber Coalition – the international cyber defence exercise organised by the North Atlantic Treaty Organisation – took place in 2020, for the first time in virtual form. The Czech Republic thus again contributed as much as possible to one of the largest international cyber defence exercises.

TABLE OF CONTENTS

2	FOREWORD BY THE DIRECTOR OF THE NÚKIB	16	CYBER THREATS
		16	RANSOMWARE: A CONTINUING INCREASING TREND IN SOPHISTICATED EXTORTION ATTACKS
		17	RANSOMWARE, DDOS ATTACKS AND SPEAR-PHISHING: THE THREE MOST SERIOUS THREATS OF 2020
		18	SUPPLY CHAIN ATTACKS: A THREAT WITH GLOBAL IMPACTS BUT NEXT TO ZERO OCCURENCE IN THE CZECH REPUBLIC
3	SUMMARY OF THE 2020 REPORT ON CYBER SECURITY IN THE CZECH REPUBLIC	20	TARGETS OF CYBERATTACKS
		20	CRITICAL INFRASTRUCTURE: IMPROVED SECURITY AND NO SERIOUS INCIDENT
6	LIST OF ABBREVIATIONS	21	PUBLIC SECTOR: TARGET OF DDOS ATTACKS AND PERSONALIZED PHISHING
7	2020: CYBER SECURITY IN THE CZECH REPUBLIC IN FIGURES	22	FINANCIAL SECTOR: THE HIGHEST BUDGETS AND THE ABSENCE OF SERIOUS ATTACKS
8	ABOUT THE DOCUMENT	23	INDUSTRY & ENERGY: MORE ATTACKS BUT LOW IMPACTS
9	CYBER SECURITY IN 2020 FROM THE PERSPECTIVE OF CZECH INSTITUTIONS, ORGANISATIONS, AND COMPANIES	23	HEALTHCARE: A TEMPTING RANSOMWARE ATTACK TARGET
13	CYBER INCIDENTS FROM THE PERSPECTIVE OF THE NÚKIB	24	EDUCATION: INCREASING CYBERATTACKS
15	THREAT ACTORS IN CYBERSPACE	25	DIGITAL SERVICES: SUFFICIENT FUNDING AND LEGAL EXPERTISE

26 MEASURES

- 26 TIMELINE OF THE NÚKIB'S ACTIVITIES IN COMBATING THE COVID-19 PANDEMIC
- 27 NATIONAL CYBER SECURITY STRATEGY: AN IMPORTANT MILESTONE IN 2020
- 27 LEGISLATIVE FRAMEWORK: SETTING BASIC RULES FOR IMPORTANT ENTITIES
- 28 THE NÚKIB'S SUPERVISORY ACTIVITIES IN 2020
- 29 CYBER SECURITY EXERCISES: GREAT INTEREST, LIMITED OPPORTUNITIES
- 30 AWARENESS-RAISING AND EDUCATION IN THE CZECH REPUBLIC: THE ONLINE YEAR 2020
- 31 INTERNATIONAL COOPERATION: GROWTH OF THE IMPORTANCE OF CYBER SECURITY AT EUROPEAN LEVEL

34 TRENDS AND OUTLOOK FOR CYBER SECURITY IN THE CZECH REPUBLIC FOR 2021 AND 2022

35 SUMMARY OF ANNEXES

- 35 ANNEX 1: REPORT ON THE FULFILMENT OF THE ACTION PLAN FOR THE NATIONAL CYBER SECURITY STRATEGY FOR 2015 TO 2020
- 35 ANNEX 2: EVALUATION OF THE ACHIEVEMENT OF THE OBJECTIVES FROM THE NATIONAL RESEARCH AND DEVELOPMENT PLAN FOR 2020

37 SOURCES

LIST OF ABBREVIATIONS

ACS – Act on Cyber Security
AFCEA – Armed Forces Communications & Electronics Association
CERT – Computer Emergency Response Team
CFC – Cyber Forces Command
CI – Critical infrastructure
CII – Critical information infrastructure
CyCLONe – Cyber Crisis Liaison Organisation Network
DCS – Decree on Cyber Security
DoS/DDoS – Denial of Service/Distributed Denial of Service
DPRK – Democratic People’s Republic of Korea
EU – European Union
IIS – Important information system
ITU – International Telecommunication Union
ISVS – Public Administration Information System
MFA – Ministry of Foreign Affairs
NAKIT – National Agency for Communication and Information Technologies
NATO – North Atlantic Treaty Organisation
NCOC – National Cyber Operations Centre
NCSC – National Cyber Security Centre
NIS – Network and Information Security
NÚKIB – National Cyber and Information Security Agency
OECD – Organisation for Economic Co-operation and Development
OES – Operator of an essential service
OSCE – Organisation for Security and Co-operation in Europe
PRC – People’s Republic of China
SIEM – Security Information and Event Management
TACR – Technology Agency of the Czech Republic
UN – United Nations

2020: CYBER SECURITY IN THE CZECH REPUBLIC IN FIGURES

468 ^

cyber incidents reported to the NÚKIB

99 ^

of the reported cyber incidents handled by the NÚKIB

9 ^

significant cyber incidents handled by the NÚKIB

1 267 ^

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

738 ^

phishing attacks handled by CSIRT.CZ

8 073 v

cybercrimes and crimes committed on the Internet

100 v

participants of cybersecurity trainings organised by the NÚKIB

8 v

cybersecurity trainings organised by the NÚKIB

18 209 ^

trained public administration employees

120 ^

information and communication systems of the critical information infrastructure

52 ^

critical information infrastructure entities

85 ^

administrators and providers of important information systems

177 v

important information systems

56 ^

operators of essential services

61 ^

information systems of essential services

ABOUT THE DOCUMENT

At the beginning of 2021, the NÚKIB sent a questionnaire with 79 questions to entities regulated under Act No 181/2014, on cyber security and on amendments to related laws (Act on Cyber Security, hereinafter the 'ACS'), as well as to many other key institutions and organisations not regulated under 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 222 entities, including 63 public sector institutions, 24 financial institutions, 77 healthcare facilities, 14 organisations providing digital services, 12 energy sector entities, 12 industrial entities, and 20 educational institutions. The NÚKIB drew information from these materials for the 2020 Report on Cyber Security in the Czech Republic (hereinafter the '2020 RCS'). All data obtained from the questionnaires were anonymised.

EVALUATION PROCESS

The assessment of cyber security in the Czech Republic is based on an analytical process consisting of the evaluation of the data from the filled questionnaires, the findings of the NÚKIB, information provided by partners, and other available information from verified sources. The NÚKIB did not have the opportunity to check the data provided by the respondents or to verify the claims. The analytical conclusions contained in the report are based on the premise that the answers in the questionnaires were not distorted. The analytical assessment is described using probability expressions (see below).

The 2020 Report on Cyber Security in the Czech Republic does not provide an exhaustive list of cyber security activities. The goal of the document is to describe and assess the threats in cyberspace the Czech Republic faced in 2020, as well as actions taken to mitigate them.

PROBABILITY EXPRESSIONS USED IN THE 2020 REPORT ON CYBER SECURITY IN THE CZECH REPUBLIC

PROBABILITY EXPRESSIONS AND THEIR PERCENTAGE VALUES:

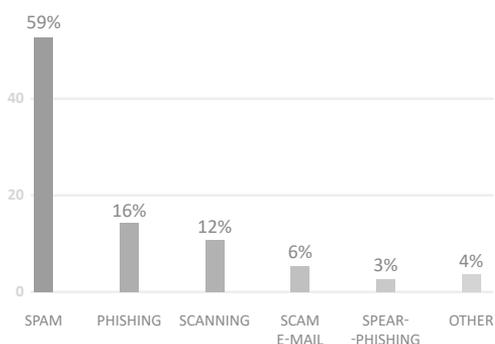
EXPRESSION	PROBABILITY
Almost certain	90–100%
Highly likely	75–85%
Likely	55–70%
Realistic possibility	25–50%
Unlikely	15–20%
Highly Unlikely	0–10%

CYBER SECURITY IN 2020 FROM THE PERSPECTIVE OF CZECH INSTITUTIONS, ORGANISATIONS, AND COMPANIES¹

INCIDENTS: AN INCREASE IN THE SEVERITY OF TARGETED PHISHING AND RANSOMWARE

According to the questionnaire respondents, the most frequent types of attacks in 2020 included spam, phishing, and the scanning of organisations' external networks² (Chart 1). On the other hand, in only a few cases did the respondents face sniffing (internal network scanning) or illegal cryptocurrency mining. The most serious attacks according to the respondents were ransomware, DoS/DDoS attacks, spear-phishing e-mails, and attempts to exploit vulnerabilities (Chart 2). Although more than half the respondents claimed they had detected at least one cyberattack attempt, such attempts did not lead to cyber security incidents in almost three-quarters of the cases, meaning the confidentiality, integrity or availability of information or services was not breached (Chart 3).³ The largest number of incidents were detected by public sphere institutions and healthcare facilities.

Chart 1: **Most frequent** types of cyberattacks in 2020 (% of respondents)



However, the fact that such a significant number of institutions did not detect a cyber security incident or

an attack attempt does not mean that no cyber incidents occurred in their networks. The ability to detect attacks targeted at data integrity and confidentiality particularly require capacities based on advanced detection technologies and sufficiently trained staff. On the other hand, detecting attacks such as spam, phishing or scam e-mails is significantly easier.

Chart 2: **Most serious** types of cyberattacks in 2020 (% of respondents)

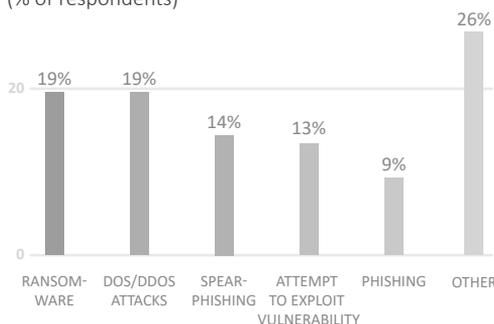
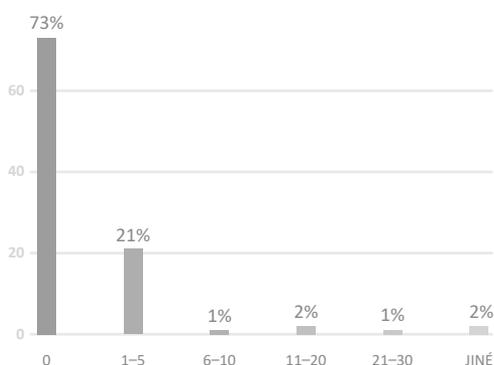


Chart 3: **Proportion of incidents with an impact on confidentiality, integrity, or information availability in 2020** (% of respondents)



1 The data follow from the evaluation of 222 questionnaires; see the section About the Document above.

2 By scanning external networks, attackers search for vulnerabilities or security flaws they can use to infiltrate the organisation in question.

3 In Europe, the mean lag between compromise and detection of a cyber security incident is 54 days, which signifies a high likelihood that, in many cases, the attacker leaves their victim's system before being detected by the victim.¹

FUNDING: A CONSIDERABLE DROP IN CYBER SECURITY FUNDING

While most respondents stated that their budget had not changed or had increased in 2019, the funds allocated to cyber security in 2020 decreased in 43% of cases (Chart 4). By contrast, the proportion of the budget spent on cyber security was comparable to 2019 and ranged between 0% and 5% of the organisation's total budget for most respondents (Chart 5). More than half the organisations considered the amount insufficient (Chart 6).

Chart 4: Development of respondents' cyber security budgets compared with 2019 (%)

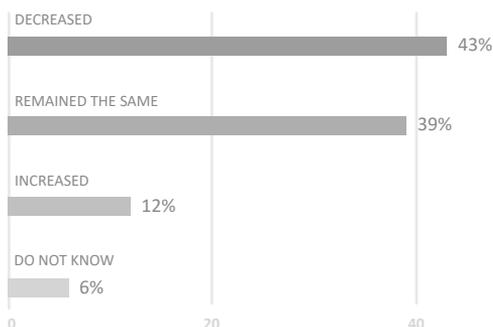


Chart 5: Share of the organisation's budget allocated to cyber security in 2020 (% of respondents)

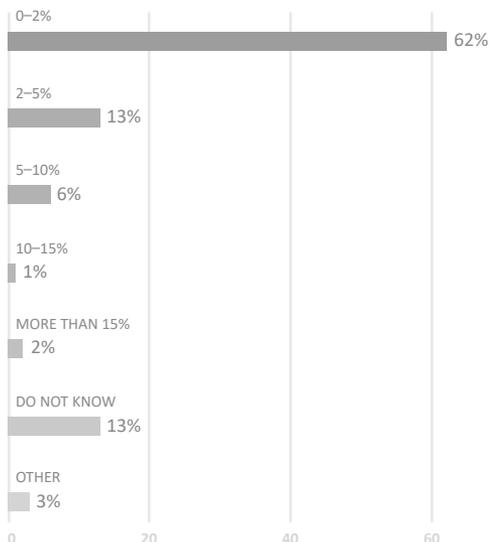
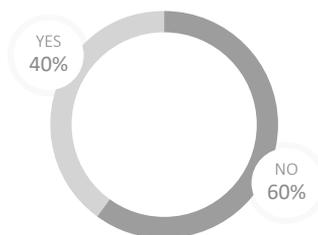


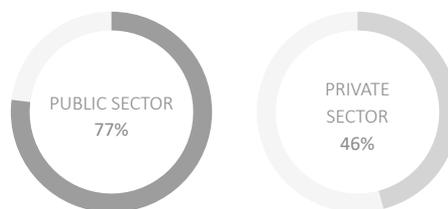
Chart 6: Did the respondents consider the funds allocated to cyber security in 2020 sufficient? (%)



PEOPLE – EXPERTS: EXPERIENCED WORKERS STAY BUT NEWCOMERS ARE DISCOURAGED BY THE FINANCIAL CONDITIONS

68% of the organisations participating in the questionnaire survey stated that low salaries discouraged new workers from cyber security jobs during the hiring process, particularly in the public sphere and healthcare. The lack of cyber security experts is a global issue. The increased demand for them means that private sector organisations are better equipped to pay higher salaries for these experts (Chart 7). In more than half the organisations, cyber security is ensured by workers with relevant work experience of 5 to 15 years or more (Chart 8). According to the respondents, cyber security architect and SIEM⁴ surveillance roles or services are the most difficult to fill in the cyber security sphere. One positive thing is that once a post is filled, the turnover of cyber security workers the organisations have to face is low. Only 10% of the respondents reported the departure of one or two employees, the main reason being other than the amount of remuneration in 74% of the cases.

Chart 7: Percentage of organisations from the public and private sectors for which the salary represented a crucial factor discouraging applicants for jobs in cyber security in 2020 (%)



4 The cyber security roles and their descriptions are taken from Decree No 82/2018, on cyber security.

As many as 38% of the respondents claimed that they had sufficient legal expertise in cyber security. Most often, the companies try to compensate for workforce shortages by outsourcing and by offering benefits in the form of further training or participation in interesting projects to attract new people (Chart 9).

Chart 8: How much relevant work experience do employees providing cyber security in the respondents' organisations have on average? (%)

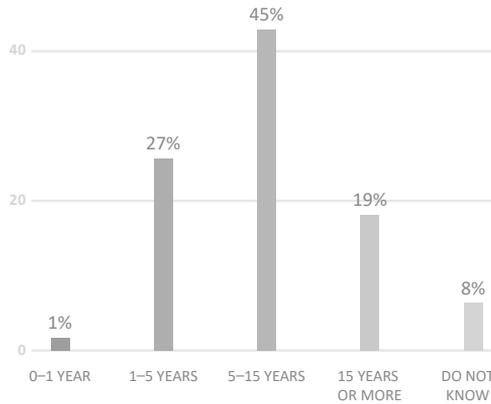
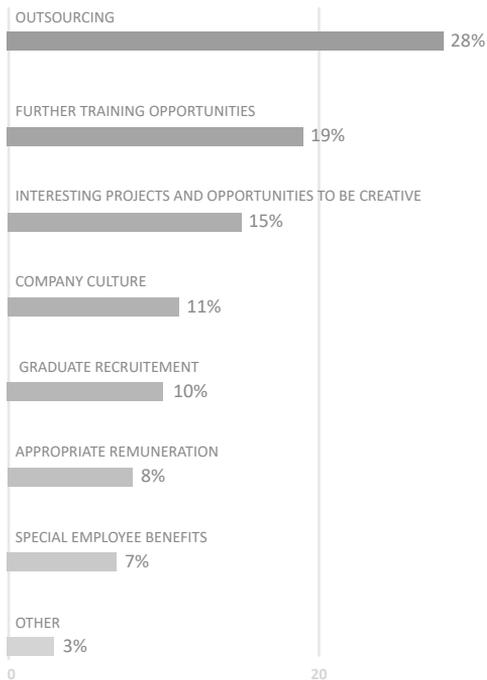


Chart 9: How did the organisations endeavour to cope with the lack of cyber security experts in 2020? (%)



PEOPLE – USERS: IMPROVING EMPLOYEE CYBER RESILIENCE BUT POOR SOCIAL NETWORK SECURITY

86% of the organisations sought to prevent cyberattacks by training their users. Although half the respondents do not specifically allocate funds to training, training took place once a year or more often in more than 50% of the companies (Chart 10). Three-quarters of such training took the form of e-learning or internal training using the company's own staff. Half the organisations also focused on other ways to improve their staff's resilience against cyberattacks. Nearly a quarter of them tested their users through simulated phishing campaigns or penetration testing (Chart 11).

Chart 10: Frequency of user cyber security training in organisations in 2020 (% of respondents)

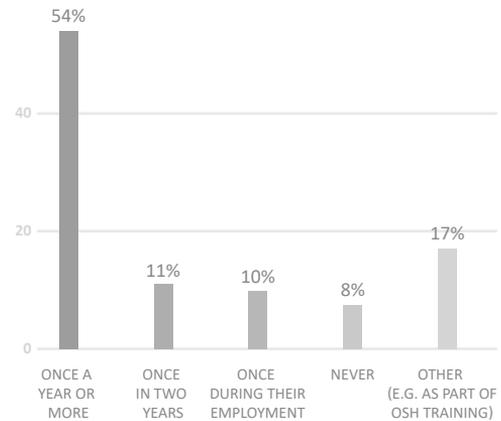
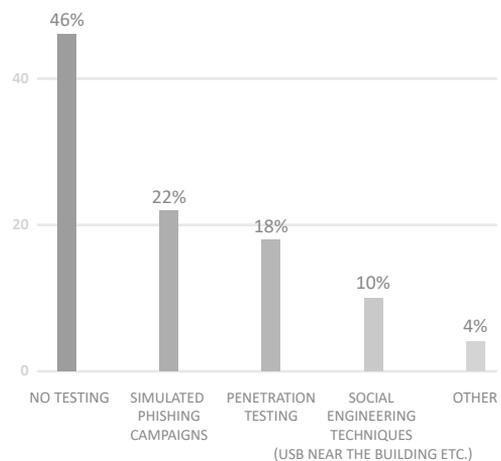
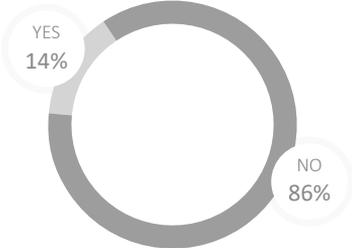


Chart 11: How employee resilience against cyber threats is tested in organisations in 2020 (%)



The organisations do not concentrate on the protection of their social networks. The questionnaire survey showed that 68% of the respondents do not use multi-factor verification despite the fact that it significantly improves digital platform security and that the misuse of a stolen account can result in reputational damages to the attacked institution. As many as 86% of the respondents have not established procedures to deal with the potential theft of accounts on social networks (Chart 12).

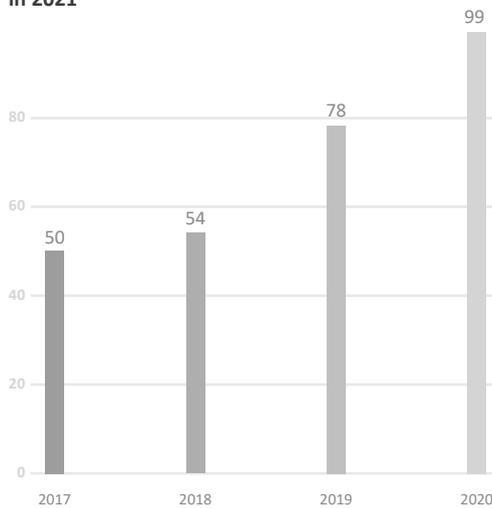
Chart 12: **If your organisation uses social networks for communication, has it established procedures to deal with the potential theft of accounts on such social networks? (%)**



CYBER INCIDENTS FROM THE PERSPECTIVE OF THE NÚKIB

In 2020, the NÚKIB received **468 notifications of cyber security incidents**, 99 of which it directly handled (Chart 13). The remaining incidents either did not require any intervention from the NÚKIB, or another relevant institution handled them. Nearly one-third of the handled incidents were reported by non-regulated entities, which represents nearly a tenfold increase compared to 2019. This increase is highly likely (75%–85% probability) caused by the higher number of cyberattacks as well as improved awareness of the existence and activities of the NÚKIB.

Chart 13: Trend in the number of cyber security incidents handled by the NÚKIB in 2017–2020: In 2020, the NÚKIB handled more incidents than in any of the past four years; we anticipate a further increase in 2021

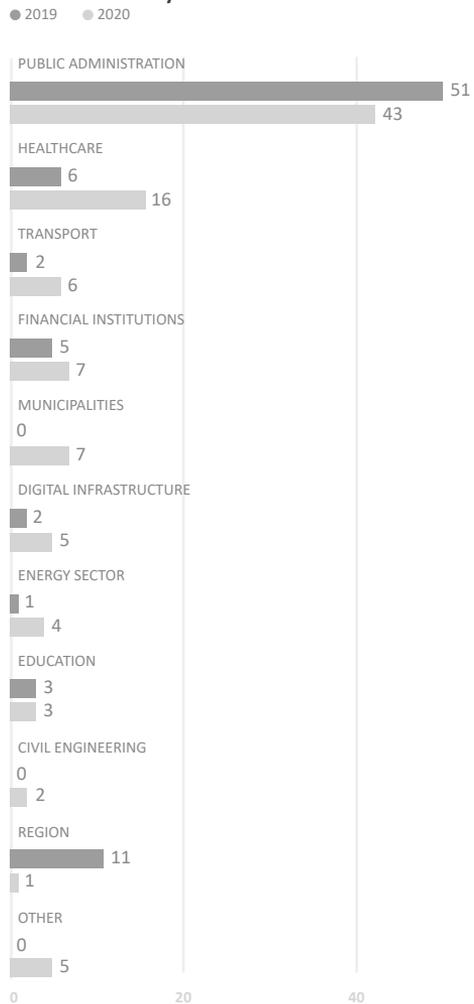


During 2020, the majority of the cyber incidents handled by the NÚKIB were in public administration (Chart 14). The second most frequently addressed sector was healthcare, where the number grew by 267% year on year. The number of handled incidents reported by municipalities also increased significantly in comparison with 2019. These increases are in line with global trends.ⁱⁱ

267%

a year-on-year increase in cyber security incidents in healthcare

Chart 14: Trend in the number of cyber incidents in 2019 and 2020 by sector



The most serious major incident handled by the NÚKIB was the encrypting of the University Hospital Brno systems using ransomware in March 2020.ⁱⁱⁱ The incident led to significant limitations on the hospital's operation at three localities and caused damage in the millions of crowns.^{iv} The Psychiatric Hospital in Kosmonosy became a ransomware victim in the same month.^v In that case, mainly the administrative infrastructure of the hospital was paralyzed but its ability to provide healthcare was not compromised, nor were any systems on which human lives depend affected.^{vi}

The third major incident⁵ of 2020 was the compromising of several dozen e-mail accounts of a strategic government institution, which occurred as a result of a successful spear-phishing campaign. Besides a breach of confidentiality of the content of the mailboxes, the compromise also caused the e-mail services to be unavailable for a day or two.

More than one-third of the incidents handled by the NÚKIB were caused by malicious code, nearly half of which through ransomware. Another almost one-third of incidents resulted in limited availability of services, systems or web portals, half of which were caused by DDoS attacks.

CYBER INCIDENTS IN 2020 BY INCIDENT TYPE

The descriptions of the categories are based on the options in the incident reporting forms:

37 MALICIOUS CODE (e.g. viruses, worms, Trojan horses, dialers, or spyware)

26 AVAILABILITY (e.g. disruption of availability caused by a DoS/DDoS attack or sabotage)

16 PENETRATION (e.g. successful compromising of an application or a user account)

7 FRAUD/PHISHING (e.g. e-mail with a malicious attachment or link)

7 PENETRATION ATTEMPT (e.g. attempt to exploit a vulnerability, compromised asset, zero day attack)

3 INFORMATION GATHERING (e.g. scanning, sniffing, or social engineering)

1 ABUSIVE CONTENT (e.g. spam, cyberbullying, inappropriate content)

2 ADMINISTRATIVE/TECHNICAL (a security incident caused by administrative or technical fault)

5 The incident severity assessment is based on Decree No 82/2018

THREAT ACTORS IN CYBERSPACE

The activities of state-sponsored actors in cyberspace and cybercrime have long been the most serious threats to the cyber security of the Czech Republic. The trend in recent years has indicated that the activities of state actors and advanced cyber threat actors have begun to overlap.^{vi}

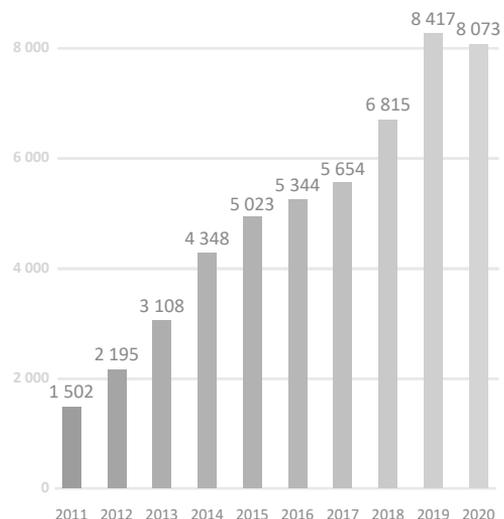
The evolution of cybercrime activities is best demonstrated by the **development of ransomware attacks**. In 2020, the healthcare sector was the most affected.^{vii} The activities of cybercrime groups in the Czech Republic were mainly visible during the ransomware attacks at the University Hospital Brno and the Psychiatric Hospital in Kosmonosy. Whereas previously extortion attacks were a non-targeted low-cost activity aimed at quick profits, the trend in ransomware activities in recent years has been characterised by a **targeting of specific institutions** rather than a random mass of individual users.^{ix} Ransomware operators preselect the institutions they consider most likely to pay a ransom. If they succeed in penetrating their systems, they do not encrypt the files immediately. Instead, they investigate the attacked system and specific data are only encrypted once their potential value for the victim has been assessed.^x **Some cybercrime groups, similarly to state actors, thus have a long-term unnoticed presence (persistence).** The expansion of Ransomware as a Service⁶ is partly responsible for this development.

The activities of state actors are extensive: from obtaining large quantities of personal data to industrial and strategic espionage, which also takes place in the Czech Republic. In 2020, the NÚKIB cooperated in the handling of an incident that involved a breach of data confidentiality in the networks of a **strategic government institution**. The NÚKIB analysis of compromising indicators discovered that the attacker was almost certainly a state actor (90%–100% probability). **The trends in espionage indicate that some states are highly likely**

(75%–85% probability) to employ cybercrime groups for espionage purposes and other state-required activities more and more often in exchange for toleration of their criminal activities.

The statistics of the Police of the Czech Republic (Chart 15) show that, contrary to their previous increasing trend, cybercrime and crimes committed on the Internet have remained at a constant level over the last two years. The number of cases investigated dropped by 4.1% between 2019 and 2020. The reason is an amendment to the Criminal Code,⁷ which increased the amount of damage that has to be caused for classification as a crime. Considering the long-term trend, a further increase in cybercrime in the Czech Republic in the coming years is likely (55%–70% probability).

Chart 15: **Cybercrime cases investigated in the Czech Republic between 2011 and 2020** (source: Police of the Czech Republic)



6 Ransomware as a Service (RaaS) denotes a service provided by ransomware developers to other hackers, usually for a share of the ransom; the ransomware developers do not take part in the actual penetration of organisations' systems.

7 Act No 333/2020, amending Act No 40/2009, the Criminal Code, as amended, Act No 141/1961, on criminal procedure (the Criminal Procedure Code), as amended, and some other laws.

CYBER THREATS

RANSOMWARE: A CONTINUING INCREASING TREND IN SOPHISTICATED EXTORTION ATTACKS

In a global perspective, the number of targeted extortion attacks grew significantly in 2020 to the detriment of large-scale ransomware campaigns. Extortion malware received maximum attention in the Czech Republic in March 2020, when the networks of the University Hospital Brno and the Psychiatric Hospital in Kosmonosy were encrypted (for details, see the chapter Cyber Incidents from the Perspective of the NÚKIB). The state enterprise Povodí Vltavy and the Prague 3 district town hall were attacked a month later. Although they occurred on the very same day, no link has been identified between the two attacks.

During the attack on Povodí Vltavy, which falls under the Ministry of Agriculture, critical information infrastructure elements were not compromised so the operation of dams and drinking water supplies was not interrupted.^{xi} The attack on the Prague 3 town hall temporarily put the operation of the CzechPoint system in its territory out of service and caused its website and several other systems to fail.^{xii} Apart from those incidents, the NÚKIB most frequently participated in dealing with the impacts of ransomware attacks in the public sector, particularly at the local and regional authorities, healthcare, industry, digital services, and education levels. **Both the number of extortion attacks handled by the NÚKIB and other verified sources indicate that the Czech Republic was also affected by the globally rising trend in ransomware attacks in 2020.**

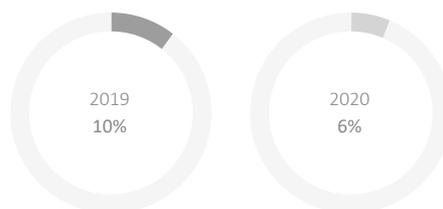
28% of the respondents faced a ransomware attack or an attack attempt in 2020. Just under one-fifth of the organisations which encountered a ransomware attack or an attack attempt classified it as the most serious, serious or moderate type of attack (Chart 16). This is a relatively low number of respondents, which might be caused by the fact that two-thirds of the organisations did not detect any ransomware attacks but more frequently faced other types of attacks, which

they subsequently considered more serious. Compared to the global boom of extortion attacks, the lower detection frequency in the Czech Republic might be due to the focus of ransomware operators on Western Europe, the Middle East, and the USA. The chances of getting the ransom paid are higher in those areas, inter alia because organisations can benefit from insurance against extortion attacks in most countries, while on the contrary, in the Czech Republic many insurance companies exclude compensation for damage caused by ransomware attacks in their terms and conditions and also reject ransom payments for ethical reasons.

28%

of the respondents said they had detected a ransomware attack or attack attempt in 2020

Chart 16: Percentage of respondents who classified ransomware attacks as most serious in 2019 and 2020 (%)



Nevertheless, institutions important for the smooth functioning of the State, such as state institutions, hospitals and energy, industrial and telecommunication companies, are also the targets of attackers. Attackers are highly likely (75%–85% probability) to continue to concentrate on them because of the higher chances of getting the ransom paid.

Besides more targeted ransomware attacks, the global trend of sensitive data theft and then repeated extortion

by threatening to make them public (so-called double extortion) continued in 2020. According to information available to the NÚKIB, no Czech institution fell victim to such an attack in 2020. However, considering the global trend, there is a realistic possibility (25%–50% probability) that the Czech Republic will be affected by this trend in the future.

Although a ransomware attack can have a serious impact on the operation of an institution, the NÚKIB recommends that attacked entities do not pay for the decryption of their data. There is no guarantee that the attacker will really do what they promise. Moreover, obtaining the money is just motivation for the attacker to attack the same institution again. In order for attacked organisations to avoid the need to consider this option, it is highly desirable to keep networks segmented, keep the operating system and applications updated, and create offline backups of at least the critical systems necessary for the operation of the institution. The answers from the respondents indicate that 56% of them create such offline backups and have implemented testing procedures, 33% of them have offline backups but do not test their recoverability, and 7% of the respondents do not create offline backups at all.

With respect to the severity and topicality of the ransomware issue, the NÚKIB issued an analysis in 2020 summarising the basic information about this type of attack, describing the fundamental vulnerabilities, and providing recommendations on how to defend against similar attacks.

The analysis is available on the NÚKIB's website: www.nukib.cz/cs/infoservis/aktuality

The supporting material Recommendations for mitigation, prevention and response, on which the NÚKIB cooperated with AFCEA and NAKIT, is available on the website at www.nukib.cz/download/publikace/podpurne_materialy

RANSOMWARE, DDOS ATTACKS AND SPEAR-PHISHING: THE THREE MOST SERIOUS THREATS OF 2020

According to organisations, the most severe threats of 2020 included ransomware and DDoS attacks (Chart 17). Almost one-third of the respondents from the healthcare sector and 25% of the respondents from the financial and public sectors considered ransomware to be the most serious form of attack. The third most serious threat was spear-phishing. In the past, potential

phishing attacks were relatively easy to detect thanks to the poor command of the Czech language and different domains in the e-mails. In recent years, however, there has been a trend towards higher sophistication of such attacks: they use better e-mail formats and an extensive portfolio of justifications, ranging from calls for invoice payments to the recovery of account access data.

28%

of organisations from the healthcare sector identified ransomware as the most serious threat of 2020

In 2020, the NÚKIB participated in dealing with the impacts of phishing campaigns as well as more targeted spear-phishing campaigns, most often against obliged entities in the public sector and, less often, the healthcare sector. Attackers most often succeeded in persuading their victims to open a file attached to an e-mail with a notification to pay an invoice. By opening the file, the user enabled macros that then caused infection with different malware.

53%

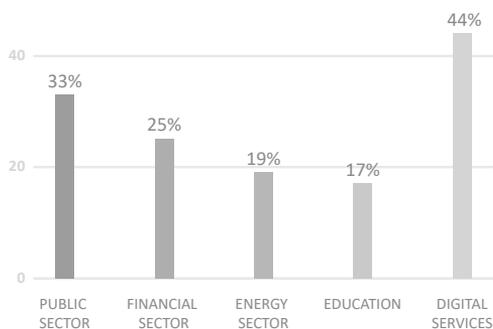
of organisations claimed that they faced spear-phishing attacks or attempts in 2020

THE RECOMMENDATIONS OF THE NÚKIB FOR DEFEND AGAINST SPEAR-PHISHING ATTACKS INCLUDES:

- Do not allow macros in MS Office documents.
- Do not automatically open attachments and links in e-mails.
- Check e-mail addresses in the case of urgent or unusual requirements.
- In the event of doubt or suspicion, contact the sender via another channel, then contact your IT department.
- Limit sharing information about job on social networks.

For more details about spear-phishing and how to defend against it, visit the NÚKIB's website at: www.nukib.cz/cs/infoservis/doporuceni

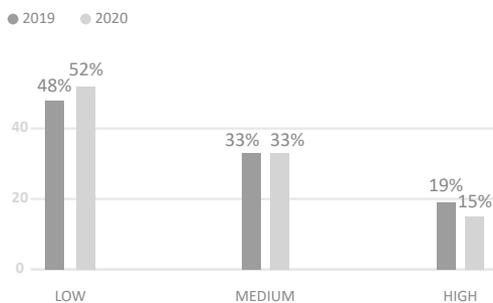
Chart 17: Share of DoS/DDoS attacks in the attacks respondents from the individual sectors identified as the most serious in 2020 (% of respondents)



SUPPLY CHAIN ATTACKS: A THREAT WITH GLOBAL IMPACTS BUT NEXT TO ZERO OCCURRENCE IN THE CZECH REPUBLIC

In 2020, less than 3% of organisations detected a supply chain attack or attempt, whereas half of them considered it the least frequent and least serious threat. This is highly likely (75%–85% probability) caused by the low occurrence of this type of attack in the Czech Republic or the difficulty for the organisations to detect it. More than half the respondents perceive the threat of cyberattacks through the supply chain as low; moreover, there has been a year on year decrease in the seriousness of this threat as perceived by the respondents (Chart 18).

Chart 18: How high was the threat of cyberattacks from a provider of services, software, or hardware in 2019 and 2020 according to the organisations? (% of respondents)



In contrast to the increasingly weak perception of the threat of cyberattacks on the supply chain in the Czech Republic, a massive attack on SolarWinds, an American software company, was detected at the end of 2020. Although the total damage is not known yet, the estimates are that there are tens of thousands of compromised⁸ clients throughout the world.^{xiii} Supply chains enable attackers to extend their attack surface in cyberspace and thus gain access to many times more sensitive data of both organisations and individuals.

The SolarWinds supply chain attack was carried out by infecting the Orion platform provided by the company with the Sunburst backdoor,⁹ which allowed the attackers to penetrate the systems of the target companies. Those included, for example, the cyber security company FireEye, the United States Departments of Treasury, Defense, and State, as well as Microsoft, Fujitsu, and Lukoil.^{xiv} In light of the seriousness of the situation, the NÚKIB issued a reactive measure, although no case of compromise has been reported from bodies regulated under the ACS so far.

REACTIVE MEASURE IN RELATION TO SOLARWINDS ORION PLATFORM APPLICATIONS

The last reactive measure of 2020 was focused on the risks associated with software from the American company SolarWinds. System administrators of critical information infrastructures, important information systems, and essential service systems immediately had to perform security updates, check whether their system had been compromised, and perform security audits.

The whole wording of the reactive measure is available on the NÚKIB's website at www.nukib.cz/cs/uredni-deska

As many as 72% of the respondents most often manage the risks associated with suppliers at contractual relationship level, which is just one of the basic measures.¹⁰ Almost three-quarters of them only grant their suppliers unrestricted remote access following the consent of the organisation's responsible person, whereas 8% of them do not grant any remote access at all (Chart 19). These results from the questionnaire survey go against

8 Clients who downloaded the malicious software update without any further consequences.

9 Backdoor denotes a method attackers can abuse to enter a system without the knowledge of the user.

10 Globally, more and more institutions are adopting the Zero Trust Security concept, in which not only the external network but also the internal network is considered untrusted and, before access is granted, all the devices attempting to connect to the organisation's networks or systems must always be verified. At the same time, users only have authorised access to services that are explicitly assigned to them, and everything else is blocked. The Zero Trust Security concept can be used to mitigate supplier-associated risks as well as to secure connections and networks for remote working.

the most frequent findings of the NÚKIB's control activities, which include insufficient management of supplier-associated risks. Apart from risk management, there is an obvious trend in authorities awarding public contracts using not only quantitative criteria, such as price, but also qualitative criteria. In 2020, the latter were used in public procurement by 61% of the respondents, mainly from the energy and public sectors (Chart 20).

Chart 19: **What level of network access do the organisations give to their suppliers?** (%)

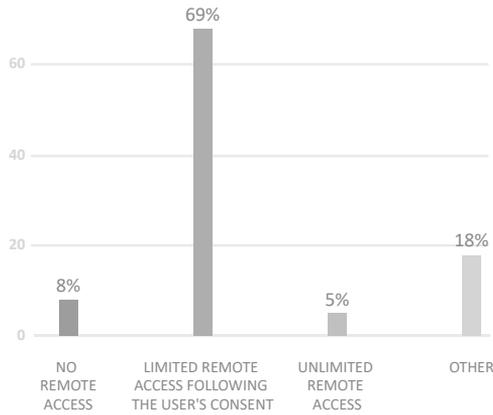
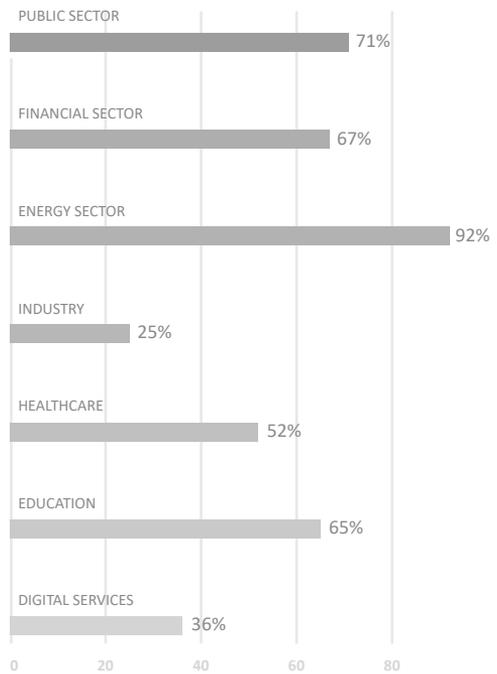


Chart 20: **Distribution of respondents (by sector) who use qualitative criteria in public procurement** (%)



TARGETS OF CYBERATTACKS

CRITICAL INFRASTRUCTURE: IMPROVED SECURITY AND NO SERIOUS INCIDENT

According to the information available to the NÚKIB, no sophisticated and targeted cyberattack compromising critical infrastructure (CI) information systems occurred in the Czech Republic in 2020.

Yet critical information infrastructure (CII) entities faced thousands of cyberattack attempts. Attacks on CII that were handled with the participation of the NÚKIB mainly occurred through DDoS attacks or attempts, while the second most frequent type of attack was phishing or spear-phishing e-mails (Chart 21). Again, the fact that no sophisticated attacks were detected by CII entities does not confirm that they are not occurring as their detection strongly depends on the technical, procedural and personal capacities of the responsible entities. Similarly to last year, nearly half the detected cyber security incidents resulted in limitations in service availability which, with CII entities, is one of the essential criteria for ensuring the smooth operation of the State and society. Mainly state administration institutions faced security incidents in relation to CII.

47%

of CII incidents reported to the NÚKIB in 2020 resulted in limited availability of services

As in 2019, one-third of the respondents categorised under CII managed to deal with the most serious attack of 2020 within several hours. In 5% of cases, the respondents were still dealing with the consequences a year later. Up to 96% of critical infrastructure organisations believe that their cyber security has improved compared to previous years (Chart 22). The NÚKIB cannot confirm this trend from information available to it. Furthermore, there is a realistic possibility (25%–50% probability) that the answers to the question were significantly affected by the positive perception of some sub-measures adopted by many of those

organisations even though these do not necessarily mean that the cyber security of the CII entities has objectively improved.

Pursuant to the ACS, critical information infrastructure (CII) consists of communication and information systems of critical infrastructure (CI) elements. Pursuant to Act No 240/2004, on crisis management and on amendments to certain other laws (the Crisis Act), CI is defined as an element or system of elements whose compromise would have a serious impact on national security, the provision of the basic living needs of the population, and ensuring the health of people or the economy of the State.

Typical CI elements include power plants, dams, airports, and telecommunication networks, as well as strategic financial institutions and State authorities. The elimination of any of these elements can paralyze the provision of critical services (energy, heat, water supplies or pension payments) or, in extreme cases (such as cyber sabotage), cause physical damage.

Chart 21: Which attacks on CII in 2020 most often resulted in a cyber security incident? (% of CII respondents)

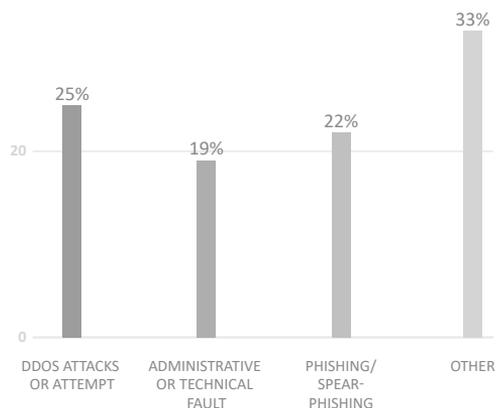
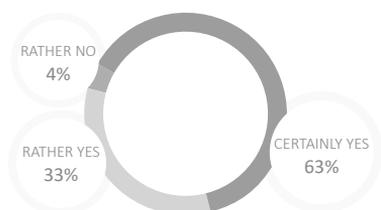


Chart 22: **According to the CII respondents, has the level of cyber security in their company improved compared to 2019? (%)**



PUBLIC SECTOR: TARGET OF DDOS ATTACKS AND PERSONALIZED PHISHING

The frequency of attacks targeted at public sector institutions increased in 2020. Moreover, the portfolio of attack types with respect to their severity has significantly changed.

The respondents' answers show that the increase in the number of attacks targeted at state administration and local and regional authorities corresponds with the data available to the NÚKIB (for details, see the chapter Cyber Incidents from the Perspective of the NÚKIB). Whereas in 2019 public sector employees most frequently encountered spam, phishing, and scam e-mails, in 2020 the institutions recorded an increase in attacks taking the form of scanning of their external networks (Chart 23). As for the severity, one-third of the respondents from the public sector and another four sectors ranked DoS/DDoS attacks highest (Chart 24). This is likely (55%–70% probability) due to the more frequent detection of this type of attack in comparison with other cyber threats. Ransomware placed second in the assessment of the severity of threats in the public sector, with one-third of the healthcare respondents considering it the most serious threat of 2020.

Chart 23: **Most frequent attacks or attempts against respondents from the public sector in 2019 and 2020 (%)**

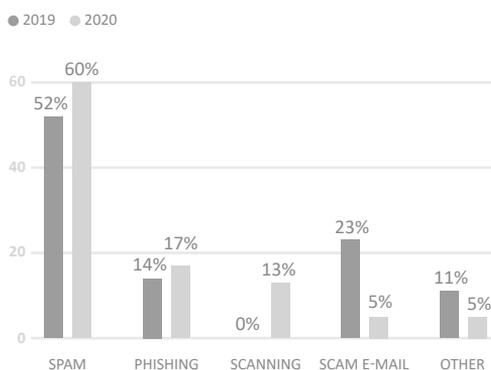
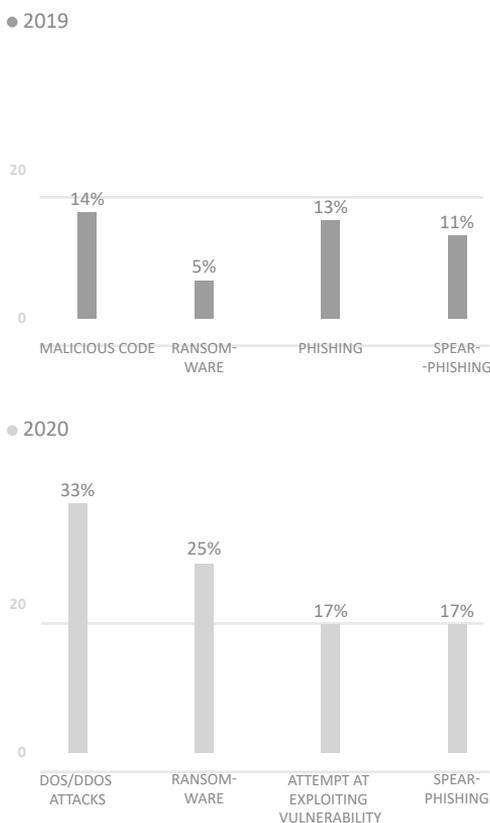


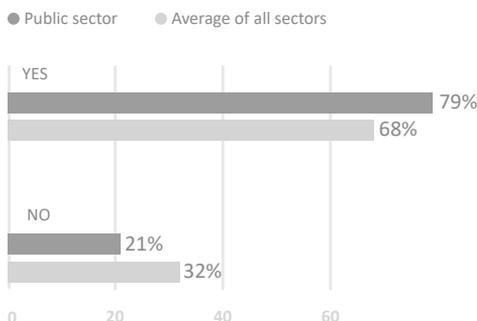
Chart 24: **Most serious attacks or attempts against respondents from the public sector in 2019 and 2020 (%)**



Similarly to last year, organisations again reported a **trend of increasingly sophisticated attacks through phishing, spear-phishing, and scam e-mails** using the pandemic or fraudulent information about parcel deliveries or overdue invoices as bait. Attackers continue to demonstrate better knowledge of both the environment and the Czech language, making it more difficult to detect them.

With public sector institutions, the **noticeable problem with hiring and paying cyber security experts** persisted in 2020. Besides this, cyber security budgets decreased in almost half the respondents from the public sector. Nearly 80% of them claimed that salaries are the main reason for the unoccupied cyber security positions (Chart 25). Despite the situation, more than half the respondents are not planning any budget increases for the coming year. The combination of these two factors could have a very negative effect on cyber security in the years to come.

Chart 25: **Were salaries the crucial factor discouraging cyber security job applicants in the public sector in 2020?** (%)



REGULATION OF THE USE OF CLOUD COMPUTING

The amendment to the Act on Public Administration Information Systems effective from August 2020 introducing new rules for the authentication of cloud computing providers and services used by public authorities represents an important advance in cyber security in the public sector. During 2021, the amendment will be further amended and completed with security rules through implementing legislation the NÚKIB is preparing in the form of decrees.

FINANCIAL SECTOR: THE HIGHEST BUDGETS AND THE ABSENCE OF SERIOUS ATTACKS

Three-quarters of the respondents from the financial sector faced cyberattack attempts in 2020. The attacks resulted in cyber incidents in only less than one-third of the cases. Although financial institutions identified targeted phishing, DDoS attacks and ransomware as the most serious cyber incidents, similarly to the year before there was an absence of more severe incidents so **the Czech financial sector can be described as relatively well secured**. Banks and insurance companies try not to underestimate cyber security as any compromising of their information systems could have far-reaching financial and reputational consequences.

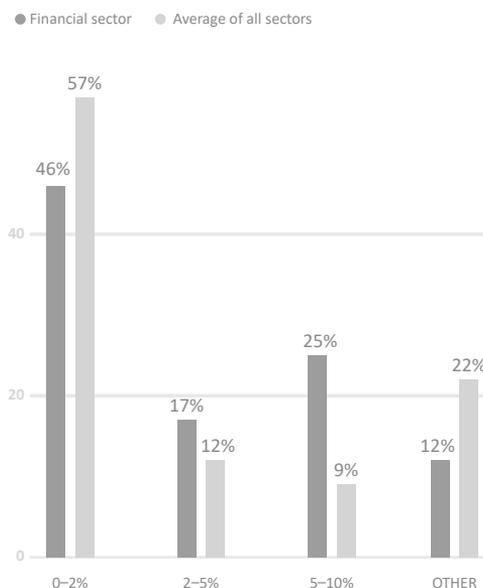
Financial institutions invest the highest percentage of their budgets in cyber security of all sectors (Chart 26) and were the only ones to state that salaries were not a fundamental factor discouraging cyber security job applicants. More than half the respondents from

the financial sector did not decrease their budgets on cyber security in comparison with 2019. On the contrary, more than a quarter of them increased their budgets. Apart from cyber security experts, all financial institutions also invest in employee training. Some organisations stated that, besides using standard methods of testing, they also planned to implement an internal Red Team.¹¹

Clients of financial institutions faced vishing (a portmanteau of voice and phishing) attacks in 2020 by which attackers tried to steal money from them. Some of the affected banks issued warnings about these vishing campaigns in which they described how such attacks are carried out.^{xv} Most often, the attackers called clients by phone, saying that their account had been attacked and recommending transferring their funds to another specific account to secure them. In some cases, they directly requested access details, including the login codes received via SMS.

Vishing campaigns are also increasing in number abroad. In 2020, American security services issued a warning about the higher frequency of this method in relation to the COVID-19 pandemic.^{xvi}

Chart 26: **What percentage of the total budgets of financial sector organisations was allocated to cyber security in 2020?** (%)



11 A Red Team is a team of ethical hackers who simulate attacks using the same sophisticated means as real attackers.

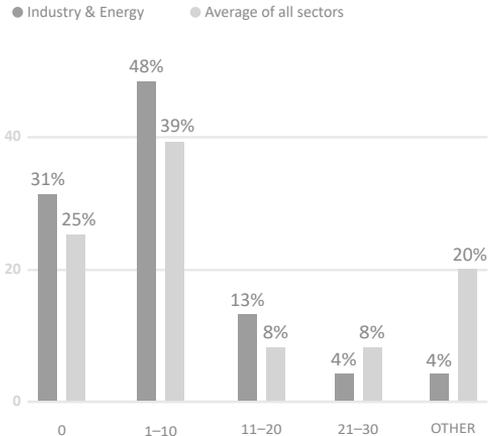
Three-quarters of the financial sector institutions have implemented BCM (Business Continuity Management) processes, thanks to which they have a system of prevention and recovery to assess the level to which they and their clients are endangered. As last year, financial institutions had the highest investments in cyber security of all the organisations questioned.

INDUSTRY & ENERGY: MORE ATTACKS BUT LOW IMPACTS

During 2020, the industry and energy sectors encountered more attacks and attempts than the average in other sectors (Chart 27). Only 4% of these resulted in cyber incidents, the impacts of which the institutions handled immediately (in almost half the cases) or within several hours. As many as 90% of the respondents consider the cyber security of their organisations fully or rather sufficient, compared to the average of 70% for all sectors.

As many as 92% of organisations in the energy sector and 58% of institutions in industry have cyber incidents incorporated in their crisis communication directive, compared to only half of organisations on average in the other monitored sectors. Although a quarter of the organisations classified supply chain attacks as serious, half the respondents stated that they were the least frequent. Even so, two-thirds of them perceive the threat of supply chain attacks on their institutions as moderate or high.

Chart 27: **How many cyberattack attempts did organisations from industry and the energy sector detect in 2020? (%)**



More than half the organisations plan to increase their cyber security budgets in the coming year, despite the fact that 54% of the respondents consider their organisation’s cyber security investments to be sufficient. At the same time, 67% of the respondents from the energy sector stated that they had sufficient legal expertise in cyber security, which is considerably above the all-sector average.

As for setting up processes, 92% of organisations in both sectors create offline backups of their critical systems and test them, and nearly half the respondents from both sectors have implemented BCM processes, compared to the all-sector average of 23%.

HEALTHCARE: A TEMPTING RANSOMWARE ATTACK TARGET

Czech hospitals and other healthcare facilities were a very attractive ransomware attack target in 2020. The focusing on such institutions can largely be attributed to the ongoing COVID-19 pandemic, which is putting high pressure on healthcare provision. Consequently, the chances of the attackers being paid the required ransom are higher. In 2020, the NÚKIB participated in dealing with nearly 20 security incidents in the healthcare sector, most often associated with phishing, ransomware attacks, and the exploitation of vulnerabilities in systems. **The most significant cases handled were those of the University Hospital Brno and the Psychiatric Hospital Kosmonosy** (for more details, see the chapter Cyber Security Incidents from the Perspective of the NÚKIB).

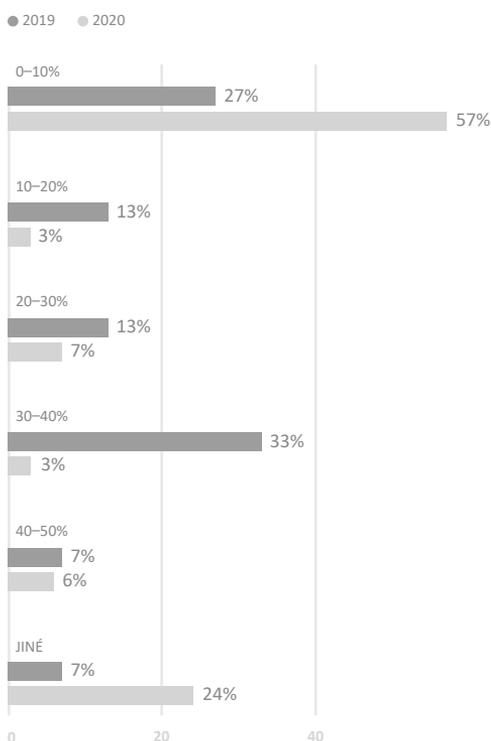
THE UNITED STATES OF AMERICA EXPRESSED CONCERN ABOUT THE ATTACKS ON THE CZECH HEALTHCARE SECTOR

In the first half of the year, Czech hospitals were exposed to a high cyberattack threat. Among others, Michael Pompeo, the then United States Secretary of State, expressed his support for the Czech Republic in combating the pandemic as well as ensuring cyber security, stating that the USA was concerned about the situation and that anybody participating in such activity had to be ready to bear the consequences of their actions. He also called upon ‘the actors in question to refrain from carrying out disruptive malicious cyber activity against the Czech Republic’s healthcare system or similar infrastructure elsewhere’.^{xvii}

Nearly 90% of the respondents from the healthcare sector believe that the level of cyber security in their organisations has improved. Nevertheless, the NÚKIB's activities in several healthcare facilities in 2020 indicate that the overall level of cyber security is still insufficient. Similarly to previous years, **three-quarters of the respondents consider the funding allocated to cyber security to be deficient.** In 2019, almost half the healthcare organisations questioned would increase their cyber security budgets by more than 100%, compared to only one-third speaking in favour of an increase of 50% in 2020.

As in previous years, salaries have remained the crucial factor discouraging cyber security job applicants for almost three-quarters of the respondents. **Compared to last year, there has been some positive development as the percentage of unoccupied posts has decreased in almost all categories** (Chart 28). It can be concluded from the respondents' answers that cyber security has come to the forefront of the budget priorities, but in most cases the respondents could only increase their budgets thanks to the 10th Call of the EU's Integrated Regional Operational Programme for Cyber Security.

Chart 28: **Unoccupied cyber security jobs in hospitals in 2019 and 2020** (% of respondents)



THE AMENDMENT TO THE DECREE ON PROVIDERS OF ESSENTIAL SERVICES IN HEALTHCARE

In reaction to the ongoing COVID-19 pandemic and the cyberattacks on the Czech hospitals, the Decree on Providers of Essential Services was amended last year in relation to the healthcare sector. The goal of the amendment was to include a greater number of hospitals among the essential service operators and to ensure their better regional distribution in order to ensure nationwide coverage. The amendment takes account of the specifics of some health services as well as of the capacity of health service providers whose substitutability in the case of outage due to a cyber incident would be difficult, and ensures connection to the integrated rescue and emergency system. The amendment took effect from 1 January 2021 and supposes that, based on the new criteria, about 30 additional hospitals should be regulated in 2021 on top of the original number of 16 most important hospitals.

The complete wording of the amended Decree is available at aplikace.mvcr.cz/sbirka-zakonu

EDUCATION: INCREASING CYBERATTACKS

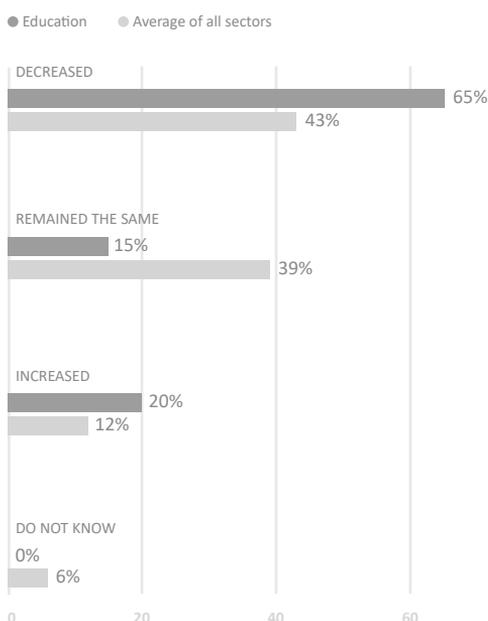
Czech academic institutions have become the targets of ransomware attacks more and more often. Throughout 2020, universities and colleges repeatedly warned against harmful practices in cyberspace targeted at their institutions. Prague University of Economics and Business faced a ransomware attack,^{xviii} Masaryk University in Brno detected new malware aimed at its users via a targeted phishing campaign^{xix}, and Palacký University Olomouc detected a previously unknown form of ransomware that encrypted all data upon a computer restart.^{xx} **The increase in attacks against Czech educational institutions mimics the global trend.**

As in the previous year, the most serious cyberattacks in absolute figures according to the educational institutions were phishing campaigns – from simple, widespread ransom e-mails to sophisticated and specifically targeted scam e-mails, in which the attackers pretended to be employees of the university. One-fifth of the respondents ranked ransomware second of the most serious threats.

One way in which the institutions can diminish the threat of a successful phishing attack is by training their employees in cyber security. Although three-quarters of

organisations do not specifically allocate funds to employee training, exactly half the respondents perform it. **The education sector was the most affected by budget decreases of all sectors, although 65% of respondents saw decreases** (Chart 29). More than one-fifth of educational institutions were in favour of increasing their budgets by at least 50%.

Chart 29: **How did the organisation's cyber security budget change in 2020 in comparison with 2019? (%)**



In order to minimize the threat of successful cyberattacks on educational institutions, it is primarily desirable to identify the information systems used. On 1 January 2021, the amended Decree No 317/2014, on important information systems and their determination criteria entered into force, under which information systems of colleges and universities may also fall.

More details are available in the NÚKIB supporting materials, such as the Guidebook to IIS identification on the NÚKIB website: www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy

DIGITAL SERVICES: SUFFICIENT FUNDING AND LEGAL EXPERTISE

The crisis management processes of the majority of Czech institutions that provide digital services (telecommunications, digital infrastructure, internet services, etc.) include cyber incident response scenarios. In 2020, almost half the respondents dealt with one to five cyber incidents (Chart 30), of which DoS/DDoS attacks were perceived as the most serious by one-fifth of the organisations.

50%

of organisations grant their suppliers no access to their networks

Exactly half the respondents do not grant their supplier any remote access into their networks, whereas the other half grant them restricted access following the user's consent. This is presumably why 57% of the respondents perceived the threat of supply chain cyberattacks as low or very low.

In 2020, one-third of the institutions from the digital services sector spent from 5% to more than 15% of their total budget on cyber security, which is only comparable to the financial sector. Less than three-quarters of the respondents consider the amount sufficient, whereas one-third plan to increase the cyber security budget next year, which corresponds to the average of respondents' answers across the sectors. Digital service institutions, as well as industry and the energy sector, have legal expertise at a level higher than the average of all respondents.

Chart 30: **How many cyberattack attempts in the digital services sector resulted in a cyber incident, i.e. where confidentiality, integrity, or availability of information was breached? (%)**



MEASURES

TIMELINE OF THE NÚKIB'S ACTIVITIES IN COMBATING THE COVID-19 PANDEMIC

MARCH

REACTIVE MEASURES FOR SELECTED ENTITIES IN HEALTHCARE

Through a reactive measure, the NÚKIB **ordered** selected healthcare entities falling under the ACS to perform necessary operations to secure important information and communication systems against cyber security incidents. In the context of the reactive measure, a recommendation was issued and sent by the NÚKIB to the backbone hospitals appointed by the Ministry of Health.

MAY

RECOMMENDATIONS REGARDING SAFE REMOTE WORKING

Tips and recommendations for safe remote working for both companies and employees in the form of a short leaflet **published** by the NÚKIB in cooperation with other partners.

OCTOBER

NOTIFICATION ABOUT SCAM E-MAILS DISGUISED AS THE RESULTS OF COVID-19 TESTS

The NÚKIB highlighted the threat of **scam** e-mails, in which unknown attackers sent false test results with a link to download malicious code. The code would then enable the attackers to access the e-mail recipient's device.

APRIL

WARNING AGAINST THREATS OF CYBERATTACKS ON HOSPITALS AND OTHER SIGNIFICANT TARGETS IN THE CZECH REPUBLIC

A month after the issuing of the reactive measure, the NÚKIB issued a **warning** against a cyber threat consisting of the implementation of an extensive campaign of severe cyberattacks on information and communication systems in the Czech Republic, and on systems in healthcare facilities in particular. The NÚKIB completed the warning with a recommendation focusing on technical and organisational issues and specified the procedures defined in the warning.

NOTIFICATION ABOUT THE RISKS OF ONLINE CONFERENCE SERVICES

Taking into account the increased need for on-line communication, the NÚKIB **pointed out** the risks associated with the use of audio and video communication services, and drew particular attention to vulnerabilities in the Zoom service, which became a frequent target of attacks.

JULY

ISSUING OF THE DOCUMENT MINIMUM SAFETY STANDARDS FOR SECURING SMALL-SCALE ORGANISATIONS

In cooperation with NAKIT and the Ministry of the Interior of the Czech Republic, the NÚKIB prepared a **document** whose goal was to assist organisations that do not fall under the ACS – typically local authorities, healthcare facilities, schools, and private companies – with their cyber security.

SECURE VIDEO CONFERENCING HANDBOOK

This **handbook** issued in cooperation with NAKIT contains essential safety recommendations and tips for secure video conferencing.

NATIONAL CYBER SECURITY STRATEGY: AN IMPORTANT MILESTONE IN 2020

In November 2020, the Government of the Czech Republic approved the National Cyber Security Strategy for the following 5 years, which was prepared by the NÚKIB. The document describes the main principles of cyber security in the Czech Republic, defines its strategic direction in cyber security, and describes the fundamental visions in this increasingly important area.

The document is divided into three main pillars, each to be fulfilled through strategic goals.

- 1. IN CYBERSPACE WITH CONFIDENCE:** Since the risk to the Czech Republic from cyberspace has been increasing over recent years, the Czech Republic must react to a whole range of new challenges. The Czech Republic should strengthen its prosperity through a confident and responsible approach to cyber security at national level. It will thus also remain a strong ally for its partners at international level.
- 2. STRONG AND RELIABLE ALLIANCES:** The flagship vision for the Czech Republic as a modern European country is an active role in creating international dialogue, and in the Euro-Atlantic area in particular. The Czech Republic will proceed from coherent national positions and clearly defined strategic interests. On this basis, it will continue to create and deepen strong alliances with its partners in cyber security and defence.
- 3. RESILIENT SOCIETY 4.0:** The Czech Republic is among European leaders in spreading and using modern technologies. As a result, Czech society is successfully transforming into an information society. This trend, however, is bringing with it not only an increase in the number of end-users in Czech society but also threats to which those users are exposed. The problems associated with this include insufficient digital hygiene, insufficient media literacy, and critical thinking across society. Therefore, the Czech Republic must concentrate on successfully transforming Czech society into the so-called Society 4.0. This is the state where the entire

society is able to fully exploit the benefits of modern technologies and, at the same time, integrate them into their everyday lives in such a way that the security risks are minimized. Cyber security must thus become an integral part of the everyday lives of citizens.

The National Cyber Security Strategy of the Czech Republic is detailed in specific tasks within the Action Plan. Both documents were prepared in cooperation with the relevant entities responsible for the essential areas of cyber security for the accomplishment of the individual tasks. The NÚKIB will continually monitor, discuss, assess and coordinate the fulfilment of the individual goals.

The National Cyber Security Strategy is available on the NÚKIB's website: <https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/>

The NÚKIB Development Concept was also approved in 2020. It describes the complete range of activities that the NÚKIB currently ensures, evaluates the current situation, and describes and justifies the need for the future development of the agency within the context of the security environment, particularly as regards cyber threats.

The complete document on the NÚKIB Development Concept is available on the website at www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan

LEGISLATIVE FRAMEWORK: SETTING BASIC RULES FOR IMPORTANT ENTITIES¹²

AMENDMENT OF THE DECREE ON IMPORTANT INFORMATION SYSTEMS

During the last year, the NÚKIB worked on an amendment to the Decree on Important Information Systems, the aim of which was to simplify and clarify the process of identification of such systems and reinforce the legal certainty of its addressees through its increased effectivity. The amendment entered into force in September 2020 and gradually came into effect from 1 January 2021. Due to the costs which will be required to secure the newly identified systems, the effectiveness of the list of systems was spread over three years.

¹² Pursuant to Act No 181/2014, on cyber security and on amendments to related laws, as amended, it includes entities whose information systems are important for the functioning of the State.

ESTIMATED INCREASE IN THE NUMBER OF IMPORTANT INFORMATION SYSTEMS DUE TO THE AMENDMENT OF THE DECREE ON IMPORTANT INFORMATION SYSTEMS

PERIOD	NUMBER OF NEWLY IMPLEMENTED SYSTEMS
2021	360
2022	260
2023	80
Total	700

CORRECTIONS AND AMENDMENTS TO LEGAL PROVISIONS

At the beginning of 2020, the ACS was amended with respect to the provisions related to offences and fines resulting from them. The amendment corrected a condition that had persisted since 2017 when some offences overlapped and some lacked any possibility of imposition of a fine.

NUMBER OF OBLIGED ENTITIES BY THE END OF 2020:

52	entities: administrators and operators of critical information infrastructure information and communication systems
120	critical information infrastructure information and communication systems
85	entities: administrators and operators of important information systems
177	important information systems
56	entities: administrators and operators of essential services information systems
61	essential services information systems

THE NÚKIB'S SUPERVISORY ACTIVITIES IN 2020

Regarding control and audit activities, 2020 was negatively affected by the pandemic, which resulted in a lower number of controls and audits performed. In 2019, the NÚKIB performed 15 controls under the ACS, whereas in 2020 it only performed **8 controls and audits** under the ACS, or Decree No 82/2018, on cyber security (hereinafter the 'DCS'). Controls and audits at obliged entities under the ACS verify that the obligations resulting from the ACS and DCS have been fulfilled. There are about 150 check points within each control or audit. **The NÚKIB's priority in the area of controls and audits was the healthcare sector, particularly in the second half of 2020.**

AREAS OF INSUFFICIENCIES MOST FREQUENTLY IDENTIFIED DURING THE CONTROL AND AUDITING ACTIVITIES:

- The set cyber security system does not cover all parties involved
- Subjects manage the assets and risks associated with cyber security inadequately
- The security policy and documentation are often not applied in practice or are not updated
- Subjects manage the supplier-associated risks inadequately
- Use of obsolete hardware and software no longer supported by the manufacturer
- Lack of cyber security experts
- Inappropriate network segmentation
- Insufficient internal network monitoring
- Too short log storage period
- Dysfunctional system ensuring the continuity of activities

COOPERATION BETWEEN THE NÚKIB AND OTHER SUPERVISION BODIES ON CONTROLS IN 2020

Last year, the NÚKIB continued in its cooperation in control activities with other regulatory bodies, with the aim of minimising the burden on the obliged entities. For example, the NÚKIB established cooperation with the State Office for Nuclear Safety via a memorandum, whereby these institutions confirmed mutual support and cooperation beyond the scope of control activities.

CYBER SECURITY EXERCISES: GREAT INTEREST, LIMITED OPPORTUNITIES

As in previous years, in 2020 the NÚKIB noticed an increased demand for exercises by Czech organisations and entities. This demand could not be completely met, however, because of the **measures associated with the global COVID-19 pandemic**. The total number of organised exercises, which are a proven tool for increasing the cyber security level, was negatively affected by the impossibility of meeting in person to discuss questions posed by a realistic scenario customized for the specific audience. Such restrictions on meetings were both on the side of the NÚKIB and the requesting subjects, which on the one hand emphasised **the safety of their employees** for logical reasons, and on the other prioritized other critical activities of their own.

Despite the above, the NÚKIB organised or coordinated **eight national and international exercises** in 2020. Apart from the representatives of the NÚKIB, **about 100 participants from various organisations actively participated** in the exercises in the Czech Republic. The exercise as part of the General Staff Course and the exercise for the Prague Castle Administration are particularly worth highlighting.

THE ADDED VALUE OF THE CYBER SECURITY EXERCISES

Exercises are an invaluable source of new knowledge, experience, and technical skills. They give the NÚKIB an opportunity to identify weaknesses in cyber security, point them out and provide an excellent tool for the verification and revision of strategies and procedures. As a tool for identification, definition and confirmation of trends, they also provide inputs for the preparation of other awareness-raising and educational activities. Furthermore, the

exercises help strengthen relations between the participants as well as with the partners cooperating with the NÚKIB on their preparation.

CYBER COALITION 2020 INTERNATIONAL CYBER SECURITY EXERCISE

This annual international exercise held by NATO, with the NÚKIB coordinating the civilian part and the Cyber and Information Warfare Command the military part at national level, saw a dramatic change compared to previous years because of the COVID-19 pandemic. The participation of the coordinating organisations and their partners was significantly limited, and the planning process and the actual exercises took place virtually. Despite the necessary adjustments to the current situation, NÚKIB representatives also managed to actively participate in the Core Planning Team responsible for the preparation and organisation of the exercises at the highest level, for the third consecutive year. **Thereby, the Czech Republic again contributed to one of the largest international cyber security exercises to the maximum extent.**

CYBER COALITION 2020 IN FIGURES



IN WHICH AREAS DO THE PARTICIPANTS TRAIN THROUGH THE CYBER COALITION?



COMM CZECH 2020 COMMUNICATION EXERCISE

The goal of the third communication exercise held by the NÚKIB was to test the availability and

up-to-datedness of the contact details provided by the obliged entities under the ACS, which are particularly important for the NÚKIB with respect to the need for **immediate crisis communication in the case of a cyber security incident**. The metrics were the availability of the contact details related to the specific systems categorised as CII, IIS or OES. Any potential unavailability or impossibility of timely communication in a real situation could result in serious damage, not only to the entity in question but in the worst-case scenario also to the whole Czech Republic. The results of the exercise were evaluated very positively as most of the contact details, and subsequently the systems, were available. The exercise also verified and confirmed that the **subjects already intensively communicate with the NÚKIB even when there is no emergency**.

IMPORTANT FINDINGS FROM EXERCISES IN PREVIOUS YEARS:

To react to serious cyber incidents in a timely, effective and adequate manner, organisations need to have cybersecurity contingency plans prepared in advance, and their employees need to know the plans.

One of the biggest cyber security challenges is the sharing of information between partners (both domestic and foreign), without which it is difficult to understand cyberattacks in a broader context and uncover all an attacker's activities, their motivation and goals, and to subsequently adopt appropriate measures.

AWARENESS-RAISING AND EDUCATION IN THE CZECH REPUBLIC: THE ONLINE YEAR 2020

The year 2020 proved that continuous and quality training in cyber security is more than important, and it has to be given maximum space. The epidemiological circumstances forced many daily activities into the online environment, and things such as home offices and distance learning became part of our vocabulary. This created not only many opportunities but also many threats, for which various target user groups had to be prepared.

The training of **public administration** users was performed via the online course **Dávej kyber! [Get Cyber Skilled!]** organised by the NÚKIB, which presents cyber security basics.

THE DÁVEJ KYBER! COURSE TOOK:

18 209 public sector employees

214 Czech Armed Forces personnel

2 000 Bulovka Hospital staff

The awareness-raising and educational activities also included the following projects for children in kindergartens to students at universities and university staff:

The expert online course **Bezpečně v kyber** [Stay Safe in Cyberspace] was taken by **1,690 prevention officers** within the scope of their professional training with a prevention extension. The course was prepared by the NÚKIB in cooperation with the Ministry of Education, Youth, and Sports and Zvolši.info, and introduces topics in online security and situations that prevention officers may encounter in the education environment.

In cooperation with the Union of Librarians and Information Workers of the Czech Republic, the NÚKIB managed to distribute the educational board game **Městečko kybernetov** for kindergartens, which presents the issue of cyberbullying and other topics to children in a soft manner.

The audio stories **Vanda a Eda v Onl@jn světě** were prepared under the auspices of the Secure Internet Festival and in cooperation with Rádio Junior and Czech Radio's (Český rozhlas) channel for children; they prepare pupils from the 1st grade of primary school for their first experience of the Internet.

The online interactive comic **Digitální stopa: Příběh Svůdčáka** was seen by **650 pupils**. It was prepared by the NÚKIB and mainly concentrates on cybergrooming for pupils of the 4th and 5th grades of primary school.

The Cyber Security Competition for Secondary School Students was held once again in the 2019/2020 school year by the Czech branch of AFCEA. Nearly **4,500 students** participated in it, 1,500 of whom qualified for the second-round runoff.

During the 2nd Secure Internet Festival, the NÚKIB distributed videos, games, and podcasts to schools via

the **Bakaláři** and **Škola Online** information systems. This meant they were offered to **280,000 users** directly on their homepages. The NÚKIB also held the **Effectiveness of Cyber Prevention** online panel discussion at the Festival, which was seen on various platforms by **4,500 viewers**. The programme presented trends and effective forms of awareness-raising in cyber security, for example.

Masaryk University opened a new **bachelor programme in cyber security**. Students will be able to study courses such as Cybercrime and cyber security or Cyber security in organisations.

1 690

workers in prevention took the
'Bezpečně v kyber' course

650

pupils read the 'Digital Footprint' comicstudents

4 500

students participated in the Cyber Security
Competition for Secondary School Students

Furthermore, significant awareness-raising and educational audio-visual materials such as films, documentaries and series dealing with various online security topics were produced in the Czech Republic last year. The following should be highlighted in particular:

#martyisdead: a thriller series on cyberbullying and manipulation prepared by Mall web-TV in cooperation with CZ.NIC and its project 'Bezpečně na netu'. The series was successful both in the Czech Republic and abroad, where it won an Emmy in the short series category.

Datová Lhota: an educational cartoon series produced by Czech Television, which presents the technical background of the Internet to children in the first stage of primary school and helps create safe behaviour habits.

V síti: a documentary that opened the issue of internet predators and stirred up a great deal of public interest.

V digitálním světě: educational videos with a similar focus for the same target group were also prepared by Jeden svět na školách, a project by the non-profit organisation Člověk v tísni.

O2 Smart School: a project by the O2 Foundation, which mainly helps pedagogues and parents to better understand the opportunities and pitfalls of the digital world.

In the area of research and development, the NÚKIB published the National Cyber and Information Security Research and Development Plan with the objective of identifying key research topics for the development of the security system of the Czech Republic. The NÚKIB also participated in the implementation of research projects dealing with the analysis of security risks associated with optical fibre networks and strategic research and development of systems for securing modern communication networks using quantum key distribution and post-quantum cryptography.

A **Junior Centrum Excellence** centre for information security at the Secondary School of Informatics, Postal Services and Finance Brno was opened at the beginning of 2020. The objective of the Junior Centrum Excellence centres is to ensure the creation of a future expert foundation that will enable better responses to the latest cyber threats. The centres are exceptional and progressive in their approach to teaching and education in information security, the implementation of safety measures and, last but not least, in their technical equipment. With their help, other secondary schools can also teach information security.

INTERNATIONAL COOPERATION: GROWTH OF THE IMPORTANCE OF CYBER SECURITY AT EUROPEAN LEVEL

The development of regulatory tools in the Czech Republic largely depends on the situation abroad as well as on the decisions adopted at European and international level. The NÚKIB represents the Czech Republic's interests in cyber security in international organisations and integration groups, namely in the EU, the UN and NATO, but also in the OECD, the OSCE and the ITU, together with the Ministry of Foreign Affairs (hereinafter the 'MFA'), the Ministry of Defence and

other partners.¹³ In 2020, Czech Republic representatives concentrated at EU level mainly on negotiations in the areas of the regulation on competence centres, the agenda of cyber security certification, the Cyber Diplomacy Toolbox application,¹⁴ the launching of the CyCLONe network,¹⁵ sounding talks on revising the NIS Directive¹⁶ and concluding discussions about the 5G EU Toolbox¹⁷ and its subsequent implementation. The Open Working Group within the UN continued with its activities, in which both the NÚKIB and the MFA actively participate.

PRAGUE 5G SECURITY CONFERENCE 2020 AND PRESENTATION OF THE PRAGUE 5G SECURITY REPOSITORY

In September 2020, the NÚKIB, the Office of the Government and the Ministry of Foreign Affairs organised the 2nd two-day Prague 5G Security Conference, a leading international forum for discussion of the risks associated with the building of 5G infrastructure. Similarly to last year, the conference was held under the auspices of Andrej Babiš, the Prime Minister of the Czech Republic. Although the conference was virtual for the first time due to the COVID-19 situation, more than 50 speakers from Europe, the USA, South Korea, Israel, Australia, India, and other countries spoke at it.

The main outcome of the 2nd conference was the presentation and launching of the **Prague 5G Security Repository**, a virtual library intended for sharing legislative, strategic, and other tools which the countries adopted in the area of 5G network security over the past year. Hence this year's conference followed on from the release of the Prague Proposals (a set of recommendations and principles countries should take into consideration when building their 5G infrastructure) of the year before.

The 3rd Prague 5G Security Conference is scheduled for autumn 2021. A key theme of the conference will be 5G infrastructure security in the context of future and

emerging technologies, including the Internet of Things and artificial intelligence.

The Prague Proposals adopted in 2019 became the basis for concluding of bilateral agreements in the 5G networks security field for many countries. Consequently, they are explicitly stated in the bilateral declarations on the 5G infrastructure security which were concluded, for example, between the USA and Estonia, Poland, Romania, Kosovo, Slovenia, Lithuania, Bulgaria, North Macedonia, and Slovakia.

THE NEW EU CYBER SECURITY STRATEGY^{xxiii} AND PROPOSAL FOR A DIRECTIVE TO REPLACE THE NIS DIRECTIVE^{xxiv}

The end of 2020 brought a new cyber 'package' prepared by the European Union with the assistance of the Czech Republic, among others. Apart from the release and gradual implementation of the 5G EU Toolbox^{xxv} and the conclusion of the discussions about the Regulation on the Cyber Security Competence Centre,¹⁸ the preparation of such fundamental documents with actual impact illustrates the importance of the close cooperation established by the Czech Republic within the European Union.

The new **EU Cyber Security Strategy** puts great emphasis on the protection of critical infrastructure, draws attention to international security and stability risks resulting from geopolitical competition between countries and hybrid threats, and highlights the importance of cyber security as the crucial aspect in people's confidence in innovations and automation.

Greater harmonisation of legal regulations and the approach of Member States to cyber security are the subject matter of the **proposal of the European Commission to replace the NIS Directive**. The new directive should adapt the coordinated detection of vulnerabilities, expand the sectors of obliged entities, unify methods for the identification of obliged entities, and establish new obligations in incident reporting.

14 In July 2020, the European Union first implemented the sanction mechanism which is a part of the Cyber Diplomacy Toolbox. Sanctions were imposed on two citizens of the PRC, four citizens of the Russian Federation, and three organisations from the PRC, Russia and the DPRK.^{xxi} This was a punishment by the EU for the Cloud Hopper cyberespionage campaign performed by the Chinese APT10 group detected in April 2017, the attacks on the Organisation for the Prohibition of Chemical Weapons (2018), the NotPetya cyberattack (2017) ascribed to Russia, and finally for the WannaCry ransomware attack ascribed to the DPRK. In October 2020, sanctions were imposed on another two citizens and one organisation from the Russian Federation.^{xxii} Identifying individuals and organisations from the respective countries does not imply any official attribution of the attacks by the EU, even though the two Russian entities were organisational units of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation GRU (also GU). The identified physical and legal persons are prohibited from entering the EU, and their funds have been frozen.

15 CyCLONe is a network of liaison organisations for dealing with cyber crises.

16 The official name is the Directive on Security of Network and Information Systems.

17 The official name is the EU Toolbox on 5G Cybersecurity.

18 Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

As unnecessarily strong as this harmonisation is in some respects in the Czech Republic's view, it represents good groundwork for negotiations on the final form of this important EU legislation.

Both documents can qualify as critical for the political and legislative anchoring of cyber security in the EU for many years to come. Their ambitiousness reflects the increasing importance of cyber security at both European and international level.

At the beginning of 2020, the Czech Republic joined a pan-European project aimed at creating a Europe-wide quantum communication infrastructure.

The prepared network will enable highly secured information transfer within the individual countries as well as between various EU countries. The envisaged communication channels are primarily intended for securing the critical information infrastructure. It is estimated that the actual quantum networks should be built and launched throughout the EU within a 10-year horizon.

TRENDS AND OUTLOOK FOR CYBER SECURITY IN THE CZECH REPUBLIC FOR 2021 AND 2022

- 1. RANSOMWARE:** The use of extortion malware by which attackers encrypt the data of the attacked institutions with consequent demands for ransom will almost certainly (90%–100% probability) remain one of the most significant cyber threats in the next two years. At the same time, the trend for increasing sophistication of campaigns and targeting specific victims is highly likely (75%–85% probability) to continue. Considering the persisting pressure on healthcare facilities in 2021 and 2022, it is almost certain (90%–100% probability) that they will remain the targets of ransomware. Large-scale undertakings, public sector institutions, and educational establishments are also highly likely (75%–85% probability) to become targets.
- 2. PHISHING, SPEAR-PHISHING, AND SCAM E-MAILS:** The Czech Republic will continue to face the most severe threats from 2020 in the coming years, mainly because of the persisting possibility of exploitation of the topic of the pandemic and the development of social engineering methods, such as more sophisticated spear-phishing with the use of deepfakes. It is also likely (55%–70% probability) that the spread of deepfakes will be used for vishing (a blend of voice and phishing) more often, focusing on users as well as public institutions and, above all, financial institutions.
- 3. LACK OF CYBER SECURITY EXPERTS:** The long-term shortage of experts is a factor affecting a number of cyber security areas and trends. We can therefore assume that the outsourcing of many services associated with IT infrastructure and its securing (Security as a Service, among others) is highly likely (75%–85% probability) to grow over the coming years.
- 4. CLOUD:** The growing popularity of cloud environments is highly likely (75%–85% probability) to cause a further increase in number of cyberattacks targeted at this infrastructure. Clouds will face attacks more and more frequently since both State actors and cybercrime groups will try to gain access to sensitive data or trade secrets. Insufficiencies in security (such as inappropriate configuration) are likely (55%–70% probability) to remain the most exploited vector of attacks on cloud services. There is a realistic possibility (25%–50% probability) that Czech organisations or companies will be among the affected clients of those services.
- 5. CYBERATTACKS AGAINST STRATEGIC STATE INSTITUTIONS:** Central government authorities of the Czech Republic are highly likely (75%–85% probability) to face serious cyberattacks from sophisticated actors in 2021 and 2022. The public sector, including its strategic institutions (the central government authorities in particular), is a frequent target of both cyber criminals and State actors because of its visibility and access to sensitive information. Foreign cases (such as the SolarWinds case) demonstrate that attackers are using more and more sophisticated methods to enter their victim's system and the attacks are consequently more difficult to detect. Based on the above-mentioned facts, its own data, and information from its partners, the NÚKIB estimates that the trend of serious cyberattacks against strategic government authorities will materialise in the Czech Republic in the next two years, and one or more of them are highly likely (75%–85% probability) to face a serious cyberattack from sophisticated actors.

SUMMARY OF ANNEXES

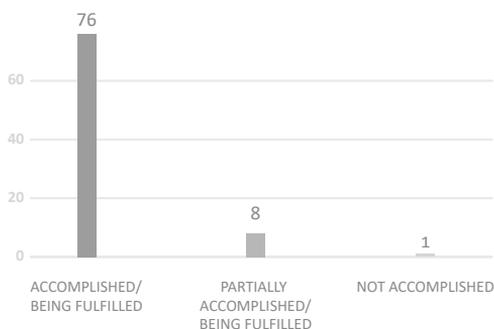
ANNEX 1: REPORT ON THE FULFILMENT OF THE ACTION PLAN FOR THE NATIONAL CYBER SECURITY STRATEGY FOR 2015 TO 2020

The year 2020 was the closing year for the fulfilment of the Action Plan for the National Cyber Security Strategy of the Czech Republic for 2015 to 2020 (hereinafter the 'Action Plan'). A substantial part of the tasks were evaluated as accomplished or being fulfilled. The number of ongoing tasks has grown compared to the previous year due to the COVID-19 pandemic. These tasks were only partially accomplished because of the epidemiological measures, which significantly affected activities requiring cooperation. For example, the ongoing tasks in the area of cyber exercises whose performance was either cancelled or postponed were assessed as partially accomplished. The situation was similar in the area of educational activities, some of which were directly cancelled, postponed, or transformed into online form.

The fulfilment of tasks that were wholly or partially accomplished in the past was also evaluated. One of these was the creation of an automated platform for sharing information about cyber threats under the competence of the NÚKIB. The platform was being developed during 2020 as part of the Non-public Web project, beta testing of which has been in progress since the beginning of 2021. Since mid-February 2021, entities regulated under the ACS as well as partners of the Government CERT have been gradually connected to it.

Only one of the assigned tasks had a fixed deadline in the given year, namely the Full Provision of Cyber Defence of the Czech Republic through the cooperation by the NCOC,¹⁹ the NCSC, the national CERT, and other CERT/CSIRT-type workplaces. This task, managed by Military Intelligence, was evaluated as partially accomplished because of the postponing of the approval of necessary legislative changes required for the full-fledged cyber defence of the Czech Republic, and its complete accomplishment has been postponed to 2022.

Chart 31: Evaluation of the tasks from the Action Plan for 2020



ANNEX 2: EVALUATION OF THE ACHIEVEMENT OF THE OBJECTIVES FROM THE NATIONAL RESEARCH AND DEVELOPMENT PLAN FOR 2020

In the area of research and development, the NÚKIB released the National Research and Development Plan, aiming at identifying the key research topics for the development of the security system of the Czech Republic. It includes the following topics:

- 1. Priority research topics shall be incorporated in public tenders and national and international research, development and innovation support programme calls.** At the end of 2020, the NÚKIB started collecting information to draw up a list of research needs in order to submit them under the Programme for Security Research for State Purposes for 2022–2027. Under this objective, the NÚKIB supported the efforts of the Ministry of Defence of the Czech Republic to strengthen research and development cooperation in cyber security and defence.

EVALUATION: Considering the short-term horizon, it cannot yet be evaluated whether the

19 The NCOC is the successor to the National Centre of Cyberspace Operations (NCCO).

number of implemented projects has increased compared to 2019.

2. **Greater involvement of the user community in the system of support for research, development and innovation (also referred to as R&D&I) in cyber security, including enhancing the capacity to deploy results in practice.**

In 2020, the NÚKIB participated in two research projects focused on security risk analysis for fibre optic networks and strategic R&D for systems to secure modern communication networks using quantum key distribution and post-quantum cryptography. The NÚKIB has applied for membership in the TACR – BETA2 programme board.

EVALUATION: Compared to 2012, the NÚKIB increased its involvement in R&D&I projects funded from national programmes, but it is not possible to assess the extent to which the NÚKIB contributes to putting the results of R&D into practice due to the short period of time.

3. **The NÚKIB as an information and analytical foundation in R&D&I in cyber security.**

The ‘Research and New Technologies in Cyber and Information Security’ and ‘News in Cyber Security R&D’ newsletters on the NÚKIB website are regularly updated. At the end of 2020, the NÚKIB prepared the summary report ‘Trends in Cyber and Information Security in the Czech Republic for 2020–2023’, which was submitted to partners in the security community.

EVALUATION: The NÚKIB succeeded in starting a process for regularly updating its partners on the possibilities of financing research projects, news in R&D&I, and opportunities to participate in research consortia.

4. **Developed international cooperation.**

In 2020, the NÚKIB continued to support project consortia under the Horizon 2020 and Connecting Europe Facility (CEF) programmes. The support included six projects in total. Furthermore, the NÚKIB encouraged the Czech Republic’s joining of the pan-European EuroQCI project aiming at building Europe-wide quantum communication infrastructure.

EVALUATION: The accomplishment of this objective was significantly affected by the COVID-19 pandemic and hence was only partially accomplished. The low level of the NÚKIB’s involvement in international research projects is largely influenced by the lack of in-house capacity.

5. **The Czech Republic actively participated in joint R&D in cyber security at EU level.**

The NÚKIB participated the comments procedures for the new Horizon Europe and Digital Europe European agendas. Concerning the creation of the National Coordination Centre in the Czech Republic, the NÚKIB prepared national positions on the Proposal for a Regulation establishing the European Cyber Security Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. The NÚKIB actively participated in setting the parameters for the 2021–2027 programme period, namely for the IROP – the Cyber Security Call, Recovery Fund and ReactEU. The NÚKIB has taken the necessary steps in the area of the EU cyber security certifications to ensure the implementation of the Act on Cyber Security in the Czech legal system.

EVALUATION: With respect to all activities, the NÚKIB considers the goal accomplished.

SOURCES

- i FireEye. 2020. M-TRENDS. <https://content.fireeye.com/m-trends/rpt-m-trends-2020>
- ii GCN. 2020. Cyberattacks on state, local government up 50%. <https://gcn.com/articles/2020/09/04/cyberattacks-state-local-government-climbing.aspx>
- iii Aktuálně.cz. 2020. Na nemocnici v Brně zaútočil vyděračský virus, špitál povolal krizového IT manažera. <https://zpravy.aktualne.cz/domaci/na-nemocnici-v-brne-zautocil-vyderacsky-virus-spital-povolal/r~ff91a02c6aa011eab1110cc47ab5f122/>
- iv E-government. 2020. Zkušenosti z kybernetických útoků na sektor zdravotnictví. <https://www.egovernment.cz/soubor/zkusenosti-z-kybez-utoku-adam-kucinsky-nukib/>
- v iRozhlas. 2020. Počítače v Psychiatrické nemocnici Kosmonosy ochromil kyberútok. Péče o pacienty není ohrožena. https://www.irozhlas.cz/zpravy-domov/pocitace-nemocnice-psychiatrie-kosmonosy-kyberutok-nukib_2003301855_aur
- vi Aktuálně.cz. 2020. Další kybernetický útok za nouzového stavu: Hackeři napadli psychiatrickou nemocnici. <https://zpravy.aktualne.cz/domaci/kosmonosy-utok-koronavirus/r~188929ec732511ea9d74ac1f6b220ee8/>
- vii Bank Info Security. 2018. Cybercrime Groups and Nation-State Attackers Blur Together. <https://www.bankinfosecurity.com/cybercrime-groups-nation-state-attackers-blur-together-a-11141>
- viii IT Security. 2021. Healthcare Cyberattacks Doubled in 2020, with 28 % Tied to Ransomware. <https://healthitsecurity.com/news/healthcare-cyberattacks-doubled-in-2020-with-28-tied-to-ransomware>
- ix TREND MICRO. 2020. Boosting Impact for Profit: Evolving Ransomware Techniques for Targeted Attacks. https://www.trendmicro.com/en_us/research/20/i/boosting-impact-for-profit-evolving-ransomware-techniques-for-targeted-attacks.html
- x Unit 42, Paloalto Networks. 2021. 2021 Unit 42 Ransomware Threat Report. **2021 Unit 42 Ransomware Threat Report (paloalto networks.com)**
- xi České noviny. 2020. MZe: Na Povodí Vltavy zaútočili hackeři, přehrady nejsou ohrožené. <https://www.ceskenoviny.cz/zpravy/mze-na-povodi-vltavy-zautocili-hackeri-prehrady-nejso-ohrozene/1876968>
- xii Lupa. 2020. Počítačové systémy radnice Prahy 3 vyřadil malware. <https://www.lupa.cz/aktuality/pocitacove-systemy-radnice-prahy-3-vyradil-malware/>
- xiii Catalin Cimpanu. 2020. Microsoft says it identified 40+ victims of the SolarWinds hack. <https://www.zdnet.com/article/microsoft-says-it-identified-40-victims-of-the-solarwinds-hack/>
- xiv David E. Sanger, Nicole Perloth a Eric Schmitt. 2020. Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit. <https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html>
- xv Komerční banka. 2020. Upozornění Vishing (8. 10. 2020). <https://www.kb.cz/cs/o-bance/novinky/bezpecnost/upozorneni-vishing-8-10-2020>
- xvi Krebs On Security. 2020. Cyber Criminals Take Advantage of Increased Telework Through Vishing Campaign. **Cyber Criminals Take Advantage of Increased Telework Through Vishing Campaign (krebsonsecurity.com)**

- xvii REUTERS. 2020. U.S. says concerned by threat of cyber attack against Czech Republic healthcare. <https://www.reuters.com/article/us-czech-cyber-usa/us-says-concerned-by-threat-of-cyber-attack-against-czech-republic-healthcare-idUSKBN22000J>
- xviii Prague University of Economics and Business. 2020. Ransomware útok. <https://ci.vse.cz/blog/2020/02/11/ransomware-utok-11-02-2020/>
- xix Masaryk University. 2020. Warning: Masaryk University users targeted by malware. https://csirt.muni.cz/about-us/news/update_june_malware
- xx Computer Centre of Palacký University Olomouc. 2020. Objevila se nová forma ransomwaru. <https://www.facebook.com/itupol.cz/posts/1903363483128324/>
- xxi Council of the EU. 2020. EU poprvé uložila sankce za kybernetické útoky. <https://www.consilium.europa.eu/cs/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/>
- xxii Council of the EU. 2020. Nepřátelské kybernetické útoky: EU uvalila sankce na dvě fyzické osoby a jeden subjekt za hackerský útok v německém Spolkovém sněmu v roce 2015. <https://www.consilium.europa.eu/cs/press/press-releases/2020/10/22/malicious-cyber-attacks-eu-sanctions-two-individuals-and-one-body-over-2015-bundestag-hack/>
- xxiii European Commission. 2020. Společné sdělení Evropskému parlamentu a Radě: Strategie kybernetické bezpečnosti EU pro digitální dekádu <https://eur-lex.europa.eu/legal-content/CS/TXT/html/?uri=CELEX:52020C0018&qid=1533485886151&from=EN>
- xxiv European Commission. 2020. Proposal for a Directive of the European Parliament and of the Council on measures to ensure a high common level of network and information security and repealing Directive (EU) 2016/1148. <https://eur-lex.europa.eu/legal-content/CS/TXT/html/?uri=CELEX:52020PC0823&from=EN>
- xxv European Commission. 2020. Cybersecurity of 5G networks – EU Toolbox of risk-mitigating measures. <https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>

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 and cryptographic protection. It is also responsible for the implementation of the regulated public global navigation satellite system service 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 some related laws (the Cyber Security Act).

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;

providing technical support and other services, such as security verification using penetration testing techniques and providing vulnerability scans;

managing operative reactions to cyber incidents using expertise and access to information for efficient incident handling;

preparing national security standards, laws, and cyber security standards;

organising training and cyber exercises at both national and international level;

analysing trends in cyber security;

providing methodological support, education and awareness-raising in cybersecurity-related topics;

performing research and development in cyber security;

performing cyber security risk assessments and adopting relevant remedial and preventive measures;

checking compliance with the requirements of the Act on Cyber Security at regulated bodies;

representing the Czech Republic in the bodies of international organisations active in the field of cyber security; and

cooperating with public, private and academic sectors at both 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**.

