Report on the State of

Cyber Security in the Czech Republic in 2019

NÚKIB

Introduction by the NÚKIB Director

It is an honour and pleasure for me to present the seventh Report on Cyber Security in the Czech Republic on behalf of the National Cyber and Information Security Agency (NÚKIB). This report includes cyber security trends in 2019, the year under review, the most serious incidents that occurred in that period, and the measures implemented to protect Czech cyberspace and our citizens.

In 2019, there was a further increase in the number of cyberattacks against our country, some of which can be considered very serious. Many public and private institutions had to defend against such attacks and recover from the consequences. The NÚKIB dealt with 78 cyber incidents during the year. Its employees assisted the attacked state administration and local government institutions, hospitals and companies during system recovery, both through recommendations and methodological support, and physically directly at the incident sites. The NÚKIB was able to provide this support because of the teamwork, maximum effort, and professional commitment of all its employees.

Cyberspace has no geographical boundaries, and the attackers operating in it recognise no such boundaries as well. This means cyber security requires efficient international cooperation. Internationally, the Czech Republic is considered a trusted cyber security partner, and in many respects is even becoming a pioneer and leader of changes in cyberspace. The organization of an international security conference on 5G networks under the auspices of the Prime Minister of the Czech Republic was unquestionably the most important international activity by the Czech Republic in this field in 2019. The conference was attended by numerous government officials, experts from over 30 countries, and international organizations. Through the conference outputs, the Czech Republic actively contributed to the advancement of cyber security in the EU and at global level, something we are rightly proud of.

The increasing level of digitalization of our society has led in turn to ever more of our activities taking place on the internet. Breaches of security of the Czech Republic's cyberspace therefore affect all our lives. The risk of successful cyberattacks will continue to increase in the future, and it is highly likely that each of us will be impacted by a cyberattack sooner or later. This concerns not only the administrators or operators of information and communication systems that are important for key functions of the state and the functioning of our society, but ordinary citizens as well.

Cyber security requires team effort, effective communication, and cooperation by the public and private sectors, all state administration and local government authorities, the security forces, industry, academia, educational institutions, and the broader public – in other words by all of us. The Czech Republic is only able to counter cyber threats thanks to the extensive cooperation, support, and effort by all entities the NÚKIB seeks to coordinate to ensure safe cyberspace for all its citizens.

On behalf of the employees of the National Cyber and Information Security Agency, please allow me to thank all of you who support us in our joint efforts. Our foreign partners, who are essential for our success, deserve our sincere thanks as well.

I would also like to thank all 125 state administration and local government institutions, hospitals, companies, and others who contributed towards the preparation of this annual report. I believe that this report, which could not have been prepared without their help, will improve cyberspace security for all of us.

Ing. Karel Řehka

NÚKIB Director

Summary of the Report on the State of Cyber Security in the Czech Republic in 2019

01 2019 was characterized by an increase in the number of cyberattacks against institutions, organizations, and companies in the Czech Republic. In 2019, 217 incidents were reported to the NÚKIB compared to 164 incidents in 2018. There was an increase in the severity of the incidents, as illustrated by the attacks against the Hospital of Rudolf and Stefanie Benešov and the OKD mining company. The most frequent types of attacks in 2019 included spam, phishing and fraudulent e-mails, which are often the first stage of more sophisticated and harmful ones.

02 In 2019, the NÚKIB and its partners noted a case of cyber espionage against a strategic state administration institution, almost certainly conducted by a state actor. According to the NÚKIB findings, Sofacy was behind the attack, i.e. a threat actor the professional community, including the NÚKIB's partners, links to the Russian military intelligence GU (also known as GRU).

03 In comparison to 2018, there were fewer cases of cryptocurrency mining via malware. The character of ransomware campaigns changed too– the number of rather primitive indiscriminate attacks decreased but there was an increase in the number of targeted and sophisticated attacks. This became apparent at the end of the year, when the Ryuk ransomware attacked systems at the hospital in Benešov and the OKD mining company.[i]

04 Of the sectors monitored, healthcare faced the greatest shortage of cyber security experts, yet at the same time is increasingly the target of cybercriminals. In December 2019, the hospital in Benešov was the victim of a ransomware attack. As a result, hospital services were limited for almost a month and the damage caused was estimated at between CZK 40 and 50 million.

05 In 2019, many of the responding organizations faced a lack of funds in their budgets and a lack of cyber security experts as well. Virtually none of the respondents had all their cyber security positions filled. Salary conditions were the most important factor discouraging potential applicants at over half the respondents.

06 In 2019, the NÚKIB and the Ministry of Foreign Affairs together organized the first international expert conference on 5G network security – the Prague 5G Security Conference – held under the auspices of Prime Minister Andrej Babiš, who attended the conference in person. Over 150 government officials and 5G network and cyber security experts from over 32 countries, including representatives of the European Union ("EU") and NATO attended the conference. The main output of this conference was the publication of the so-called Prague Proposals, a series of recommendations on 5G network security, which were reflected in the final form of the EU Toolbox for 5G Security, and which inspired other states in the preparation of their regulatory documents.

07 In 2019, the NÚKIB continued educating state administration employees and trained over 5,000 civil servants through the e-learning course "Master Cyberspace!" ("Dávej kyber!"). The Agency further continued its awareness-raising and educational projects aimed at children, young people, and senior citizens. Awareness-raising activities were also pursued by many other organizations, including universities and telecommunications providers.

08 In 2019, the NÚKIB registered a significant increase in demand for cyber-security exercises, and held 17 of them. The Agency prepared and held, for example, a joint exercise with the **National Organized Crime Agency** and the "Electro Czech" sectoral exercise for energy industry representatives.

Table of contents

2019: Cyber Security of the Czech Republic in Figures

217 cyber incidents reported to GovCERT.CZ

78 of the reported cyber incidents handled by GovCERT.CZ

8417 cybercrime and internet crime offences

954 security incidents handled by CSIRT.CZ – the national security team of the Czech Republic

483 phishing attacks reported to CSIRT.CZ

17 cyber security exercises organized by the NÚKIB

90 countries participating in exercises

468 participants of cyber security exercises organized by the NÚKIB

5172 civil servants trained

109 critical information infrastructure information and communication systems

47 critical information structure entities

38 basic service operators

70 administrators and operators of important information systems

178 important information systems

42 basic service information systems

Chapter A

Cyber Security in 2019 from the Perspective of Czech Institutions, Organizations and Companies[1]

A | 01

Incidents:

Malware and Phishing as the Most Serious Threats

In 2019, the most frequent types of attacks encountered by the responding organizations included spam, phishing, and fraudulent e-mails (Chart 1), i.e. the least sophisticated attacks. Most respondents considered malicious code (viruses, worms, trojan horses), ransomware and phishing to be the most serious types of attacks (Chart 2). The attempted cyberattacks were not always successful. Third of the respondents suffered a breach of confidentiality, integrity or availability of information or services as a result of an attack. Most respondents reported the number of incidents as between 1 and 5 (Chart 3). The highest occurrence was reported by regional and local authorities and financial institutions. About a third of the incidents resulted in limited availability of services. Almost a third of the respondents encountered DDoS (Distributed Denial of Service) attacks, but neither the respondents nor the Agency noted any larger scale attack of this type. Likewise, neither the respondents nor the Agency noted any larger scale attacks via SQL Injection.[2]

Chart 1: **Most frequent** types of attacks in 2019 (%)

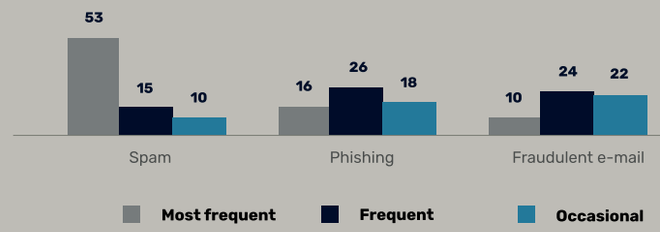
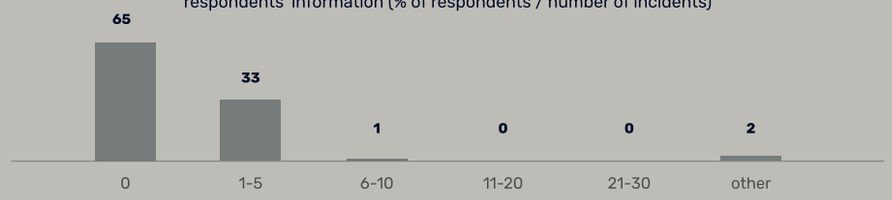


Chart 2: **Most serious** types of cyberattacks in 2019 (%)

[1] At the beginning of 2020, the NÚKIB sent a questionnaire containing 49 questions to entities regulated by Act No 181/2014, on cyber security and on amendments to related laws (the Cyber Security Act, hereinafter the "CSA"), and to many other key institutions and organizations not subject to the CSA. The questions addressed a wide range of topics, such as cyberattacks, cyber security costs, cyber security human resources, users, technologies, and established processes. The questionnaires were completed by 125 state institutions, organizations and state-owned and private companies. The NÚKIB used the data in the Report on the State of Cyber Security in the Czech Republic in 2019 (hereinafter the "2019 RCS"). All the data from the questionnaires are in an anonymized form and presented as a percentage. The following summarizes some trends.

[2] SQL Injection is a technology which exploits security vulnerabilities of the application database layer. The security vulnerability manifests itself through the infiltration of malicious code in SQL statements of an authorizer user, or in the takeover of user access for the execution of an SQL statement. The attackers can then take control of the compromised database and do practically whatever they want with it (copy, change or delete data).

Chart 3: Number of 2019 incidents with a breach of confidentiality, integrity or availability of respondents' information (% of respondents / number of incidents)



A | 02

Funds:

A Minimal Decrease in Cyber Security Budgets

The answers provided by the responding organizations indicated that a lack of funds was one of the greatest weaknesses of Czech cyber security in 2019. Most of the responding organizations allocate 0–5% of their total budgets to cyber security (Chart 4), which is considered insufficient by 44% of the respondents (Chart 5). On the positive side, cyber security budgets generally did not decrease in 2019. The budgets of 44% of the respondents increased, and of 45% remained at the 2018 level (Chart 6).

Chart 4:
Share of the total budget of responding organizations allocated to cyber security in 2019 (%)

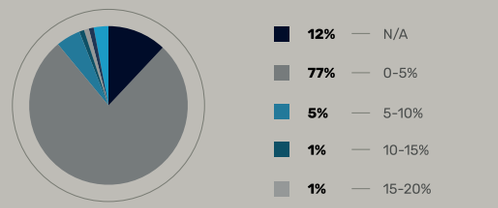


Chart 5:
Were the funds allocated to cyber security in the responding organizations sufficient in 2019? (%)

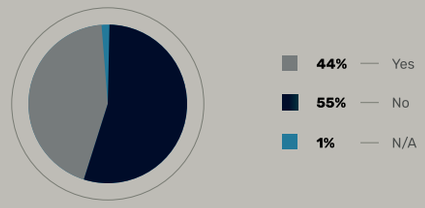
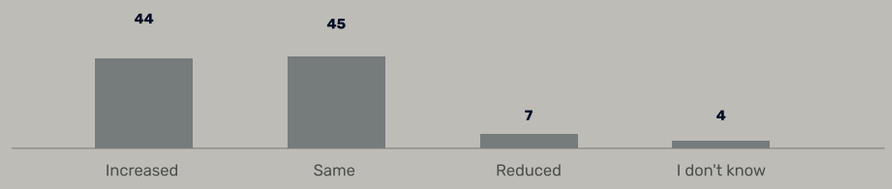


Chart 6: Development of respondents' cyber security budgets in 2019 (%)



A | 03

People – Experts:

A Lack of Cyber Security Staff

In 2019, a shortage of cyber security experts was one of the results of the lack of funds. At the end of 2019, 88% of the responding organizations needed to fill cyber security positions (Chart 7). According to 67% of the respondents, unsatisfactory salary conditions were the major reason discouraging job applicants (Chart 8). Organizations handle this situation in various ways. For example, some rely on benefits to attract applicants. Others address cyber security through various levels of outsourcing – this solution is used by half the respondents (Chart 9).

Low budgets are only one of the causes of unfilled positions. A lack of cyber security experts is a global issue, and the high demand for them results in higher salary costs than for other IT professions. This has led to a situation where only some employers, mostly from the private sector, can afford to pay enough experts. State administration, local government institutions and healthcare organizations are most impacted by this shortage.

Chart 7:

Did the respondents need to fill cyber security positions in 2019? (%)

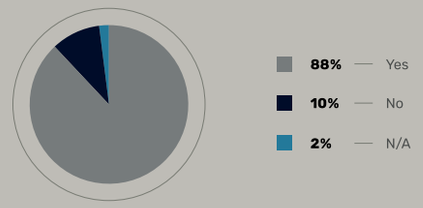


Chart 8:

Was money the major factor discouraging applicants for cyber security positions in 2019? (%)

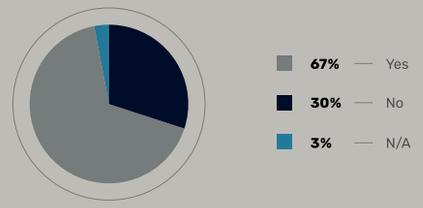
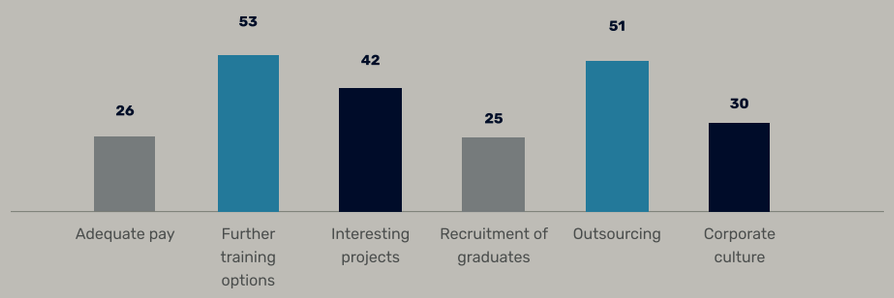


Chart 9:

How do organizations try to address the lack of cyber security experts? (%)



A | 04

People – Users:

Training as the New Standard

Users are considered the most vulnerable link in cyber security as they can disable dozens or hundreds of networked computers by merely clicking on and opening an infected attachment. In 2019, respondents' organizations took user training in existing cyber threats seriously, and the vast majority trained their users in one way or another (Chart 10). With most respondents, the training took the form of e-learning or was delivered by their own employees; a third of the organizations used third-party services in 2019. Two thirds of the responding organizations provided training at least once a year (Chart 11). Over half the respondents enhanced the resilience of their employees to cyber threats through active testing, e.g. through simulated phishing campaigns (Chart 12). The fact that users are trained by almost all the responding organizations is very positive, yet the form of training is essential in this respect. A combination of **more frequent, interactive**, and **shorter** training courses is considered the most effective.

Chart 10:

User training in cyber security in the respondents' organizations in 2019 (%)

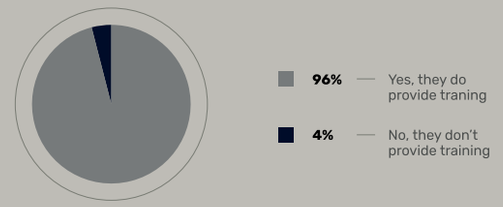


Chart 11:

Frequency of user training in cyber security in the respondents' organizations in 2019 (%)

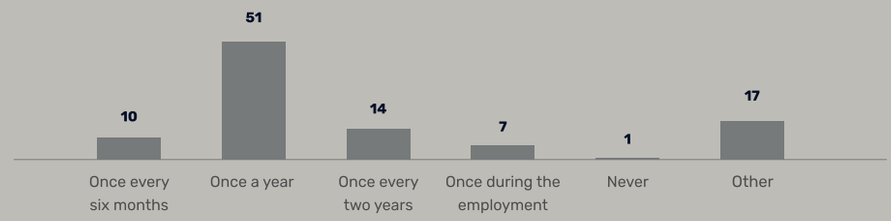
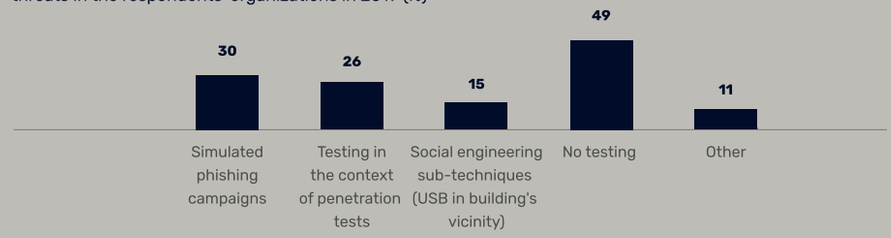


Chart 12:

Form of testing employee resilience to cyber threats in the respondents' organizations in 2019 (%)



Chapter B
Threat Actors in Cyberspace

According to the information available to the NÚKIB, cybercriminals were the greatest cyberspace threat in the Czech Republic in 2019. Another important category was comprised of attacks by foreign powers aimed at Czech state institutions.

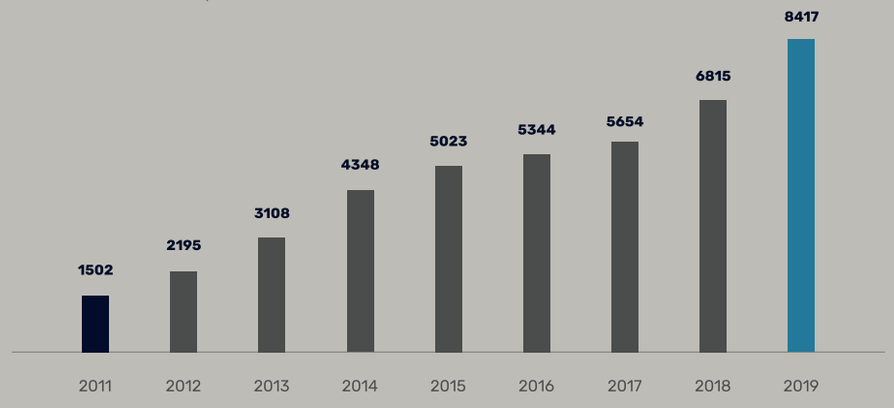
The activity of cybercriminals could be seen, for example, in the attacks on the Hospital of Rudolf and Stefanie Benešov, and OKD mining company.

As the statistics of the Police of the Czech Republic show (Chart 13), cybercrime and internet crime are on the rise **in the Czech Republic** and the number of such crimes is increasing every year. The number of cases investigated increased by 24% between 2018 and 2019. The rising trend in cybercrime has been evident for a long time, and it is highly likely (probability of 75–85%) that it will continue to grow in 2020 and 2021. The reasons behind this trend are mainly the relatively easy profits and the low risk of being caught committing the criminal activity.

Other actors active in cyberspace include cyberterrorists, politically motivated hacktivists[3], and less sophisticated actors (the so-called script kiddies[4]). None of those actors posed a significant threat to Czech cyber security in 2019.

Chart 13:

Cybercrime cases investigated
in the Czech Republic between 2011 and 2019



Source: **Policie ČR**

[3] Political activists who compromise the availability, confidentiality, or integrity of information to achieve a political, ideological or social change.
[4] Slang for amateurs who attack using tools developed by other attackers.

Chapter C
Cyber Threats

C | 01
Cyber Espionage:
Bears in the Czech Networks

As is the case almost every year, cyber espionage was a topical issue in the Czech Republic in 2019. The NÚKIB cooperated in addressing an incident which compromised data confidentiality in the networks of a **strategic state administration institution**. The initial attack vector was a spear-phishing e-mail. A subsequent analysis of compromise indicators by the NÚKIB showed that the attacker was almost certainly a state actor (probability of 90–100%) – it was highly likely (probability of 75–85%) an APT[5] **group known as Sofacy**, APT28 or Fancy Bear. The expert community, including the NÚKIB's partners, **links Sofacy** to the **Russian military intelligence GU** (also known as GRU). [iii]

In 2019, one of the most active actors in cyberspace were groups associated with the **Winnti** backdoor. Traces of Winnti could be found in cases of industrial espionage, and cyber espionage attacks on state institutions, NGOs and the media. Since its emergence, experts have linked the Winnti backdoor to the People's Republic of China (hereinafter the "PRC").[iv] In 2019, there was a large-scale attack by a Winnti group on major German companies, including Bayer, Siemens, BASF and Henkel. [v] Although the NÚKIB did not attribute any of the 2019 attacks in the Czech Republic to Winnti group, this threat **cannot be ruled out (probability of 25–50%) in the Czech Republic in the future** given the nature of the groups' targets abroad. Winnti is one of the actors that exploit weaknesses in supply chains, and has been linked by experts to the attack against the CCleaner [vi] , service bought by the Czech security company Avast in 2017 while the attack was still ongoing.

C | 02
Ransomware:
The Decline of Rather Primitive Mass Campaigns in Favour of Sophisticated Attacks

While in 2018, the NÚKIB had noted a decline of ransomware and rise of malware using the power of infected computers for cryptocurrency mining (the so-called cryptominer) in the Czech Republic, the situation was the opposite in 2019. According to security experts, 30% of organizations were infected by cryptominers in January 2019, but only 11% in October 2019. [vii] It is highly likely (probability of 75–85%) that the reason behind the decline of cryptominers is a combination of the declining lucrativeness of cryptocurrency mining and increased attention from antivirus companies.

In 2019, the number of indiscriminate WannaCry ransomware attacks decreased while, on the contrary, **the number of sophisticated targeted blackmailing campaigns increased.** This trend was also seen in the Czech Republic.

Ransomware

is a type of malware which takes the affected system and data as hostage. Attackers infect the victim's system with ransomware that encrypts all their data, and demand money to recover the data.

Despite the possible serious impacts of such attacks, the NÚKIB does not recommend that the victims pay the attackers to decrypt the data since there is no guarantee they will actually do so.

32% of the respondents stated that they had registered a ransomware attack or attempted attack in 2019

[5] Advanced Persistent Threat – designation for highly sophisticated groups of attackers.

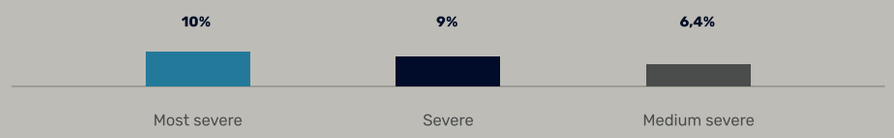
In the Czech Republic, blackmailing ransomware was most active in December 2019 in the form of a Ryuk ransomware campaign. The ransomware attacked the networks of the Hospital of Rudolf and Stefanie Benešov and the OKD mining company (for details, see the "Cyberattack Targets" chapter).

According to the data provided by the responding organizations, 32% of the respondents have encountered a ransomware attack or attempted ransomware attack, and a quarter of the respondents (Chart 14) consider ransomware to be the most severe, severe, or medium severe type of attack. These numbers are considerably higher than those in reports focused on private companies.[viii] Given the composition of the responding organizations included in the NÚKIB survey [entities subject to the Cyber Security Act (hereinafter the "CSA")], it can be deduced that it is likely (probability of 55–70%) that the Czech Republic is being targeted by sophisticated ransomware attacks. Entities subject to the CSA can be considered among the targets whose compromise might affect the smooth functioning and sovereignty of the state (state institutions, telecommunications and energy companies, and hospitals); therefore, we assume that the attackers may believe they have a better chance of being paid the ransom.

In addition to the more targeted attacks, a ransomware trend that emerged in 2019 took the form of threats to disclose sensitive data unless a ransom is paid. Such a threat puts additional pressure on the victim to pay the ransom to prevent any risk of confidential employee information or trade secrets being made freely accessible on the internet. The NÚKIB has no information indicating that any Czech organization or company fell victim to such attack in 2019, but there is a real possibility (probability of 25–50%) that the trend will hit the Czech Republic in the future.

Chart 14:

Severity of ransomware attacks according to the respondents (%)



C | 03

Phishing, Spear-phishing and Fraudulent E-mails:

Increased Quantities and Better Grammar

In 2019, phishing e-mails were encountered by 90%, spear-phishing e-mails by 44%, and fraudulent e-mails by 94% of the respondents. While phishing and fraudulent e-mails hit all sectors equally (Charts 15 and 16), spear-phishing e-mails mainly targeted financial institutions, healthcare, and other critical information infrastructure entities (Chart 17). The attackers are therefore focusing primarily on lucrative targets or entities essential for the functioning of the state, and which may potentially bring them higher profits.

There was a clear increase in phishing, spear-phishing and fraudulent e-mails in the Czech Republic in 2019, in terms of both their quantity and their sophistication. This trend was registered by 36% of the respondents. The qualitative shift was evident in particular through the more advanced Czech language used, the more sophisticated e-mail formats, and variety of e-mail motives (demands from bailiffs, minutes of a meeting etc.). In their e-mails, attackers often addressed their victims using the name of a real person, whether a colleague or a superior.

Phishing, Spear-phishing and Fraudulent E-mails

Phishing takes the form of an e-mail, SMS or social media message through which the attacker attempts to convince the victim to disclose sensitive information, open a link to a malicious website, or open a file containing malicious code. **Spear-phishing** is a personalized form of phishing, targeting specific institutions and persons. In fraudulent e-mails, attackers usually try to convince the victim to send them money. Phishing, spear-phishing and **fraudulent e-mails** are increasingly appearing on social media.

44% of the responding organizations stated that they had been subject to a **spear-phishing attack** or attempted attack in 2019

94% of the responding organizations stated that they had been subject to an attack or attempted attack in the form of a **fraudulent e-mail** in 2019

36% of the responding organizations stated that they had registered an increase in the quality and quantity of **phishing, spear-phishing and fraudulent e-mails** in 2019

90% of the responding organizations stated that they had been subject to a **phishing attack** or attempted attack in 2019

Chart 15:

Percentage of respondents (by sector) who encountered fraudulent e-mails in 2019 (%)

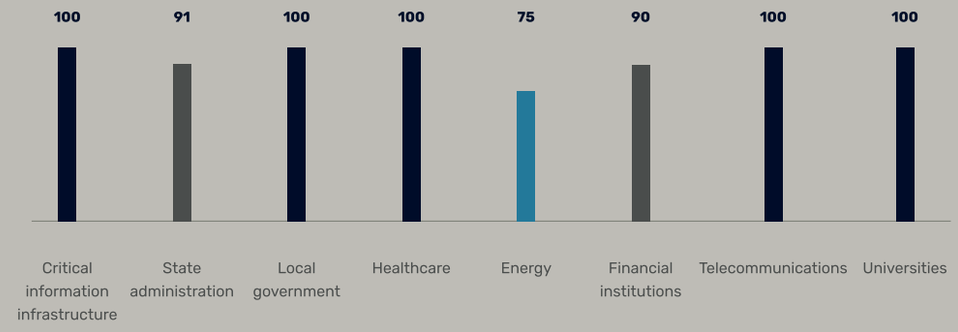


Chart 16:

Percentage of respondents (by sector) who encountered phishing attacks in 2019 (%)

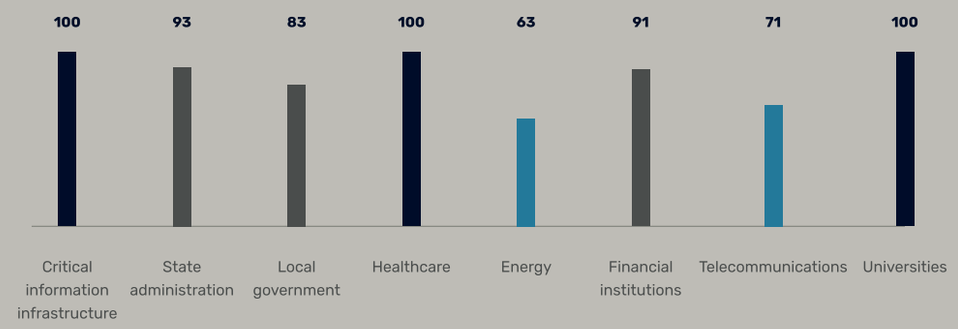
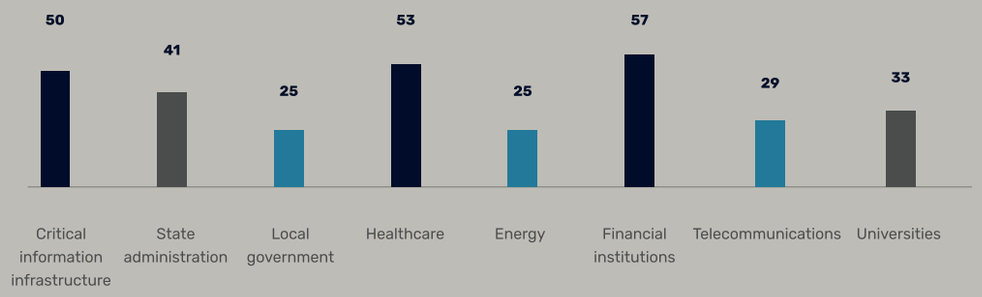


Chart 17:

Percentage of respondents (by sector) who encountered spear-phishing attacks in 2019 (%)



For more information on spear-phishing (and phishing) and how to defend yourself against it, see the NÚKIB website:

https://www.govcert.cz/cs/informacni-servis/doporuceni/2748-spear-phishing-a-jak-se-pred-nim-chranit/

The NÚKIB recommendations for protection against spear-phishing are available on the NÚKIB website:

https://www.govcert.cz/download/doporuceni/NUKIB_doporuceni-spear-phishing.pdf

In view of their increasing sophistication, it is not easy to recognize phishing and spear-phishing, something also demonstrated by the following Google test:

https://phishingquiz.withgoogle.com/

C | 04

Attacks Exploiting Supply Chain Weaknesses:

Rare but with Potentially Huge Consequences

Although only 2% of the responding organizations registered a **supply chain attack** or attempted attack in 2019, Czech institutions, organizations and companies are aware of the risk posed by this form of attack. Supply-related risks are therefore managed by 88% of the respondents (Chart 18).

The relatively sporadic occurrence of this type of attack in the Czech Republic is likely (probability of 55–70%) the reason why 38% (and therefore most) of the respondents assess the threat of cyberattacks through service suppliers as low. Only 18% assess the risk as high, while 33% assess the risk as medium (Chart 19).

Chart 18:

Did the respondents manage the risks associated with service and hardware suppliers in 2019? (%)

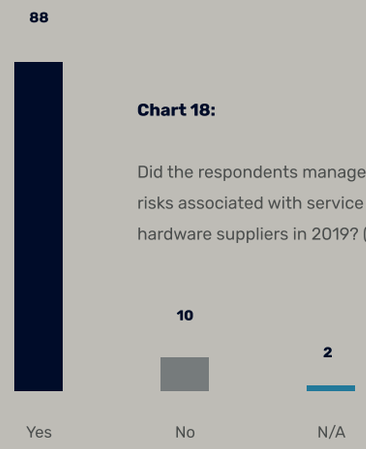
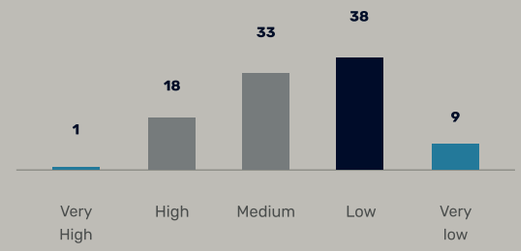


Chart 19:

Respondents' assessment of the magnitude of the threat of cyberattacks through service and hardware suppliers in 2019 (%)



Cyber security problems with the supply chain impacted the Czech Republic in 2019 too. Avast, a Czech antivirus company, fell victim to a cyberattack in the second half of 2019. The attackers got access to the company's networks, where they were subsequently detected. The attackers' goal was likely (probability of 55–70%) to infect a widely used Avast computer cleaning product – CCleaner – with malware. According to the Czech counterintelligence, Security Information Service (BIS), the 2019 attack came from China. [ix] It was already the second attempted compromise of the popular software; the first one, detected in September 2017, had been successful. An investigation carried out by an Israeli cyber security company indicated that a Winnti group was suspected of carrying out the attack. [x]

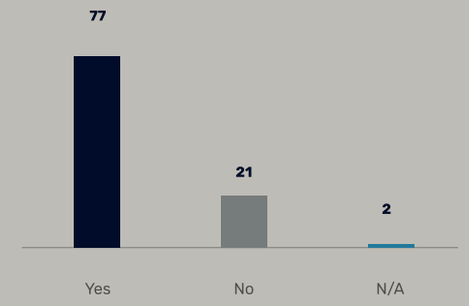
One way to manage such risks is to take into account not only quantitative aspects – such as price – in public procurement, but to consider qualitative criteria related to cyber security as well. This is done by 77% of the respondents (Chart 20). According to NÚKIB findings, the existing method of application of the Public Procurement Act (Act No 134/2016, on public procurement, as amended), where procurement procedures with the price as the main or only criterion prevail, remains a potential supply chain risk factor in the **Czech Republic.** [xi] A large number of the respondents stated that they also use qualitative criteria in public procurement (Chart 20). In 2019, the Agency furthermore registered increased interest from obliged entities in consultations regarding the awarding of specific public contracts.

In the context of the Agency's warning about Huawei and ZTE technologies, the decision by the Office for the Protection of Competition (ÚOHS) to terminate the proceedings regarding a Huawei complaint against the terms of a tender for servers for the Ministry of the Environment of the Czech Republic was an important event in 2019. Huawei had objected to the tender conditions including the NÚKIB warning, saying that it was discriminatory. The ÚOHS concluded that it did not consider the condition to which Huawei had objected to be discriminatory, since the inclusion of the condition was the only way in which the contracting authority was able to meet its legal obligations regarding cyber security.[xii]

2% of the responding organizations registered a supplier chain attack or attempted attack in 2019

Chart 20:

Do the respondents use qualitative criteria in public procurement? (%)



Chapter D
Cyberattack Targets

D | 01
State Administration and Local Government:
A Target of Sophisticated Phishing Attacks

State administration and local government institutions were frequent targets of cyberattacks in 2019. Central state administration institutions are in particular a source of intelligence, and militarily, politically, and economically relevant information for attackers linked to state actors. In 2019, state administration and local government employees most frequently encountered spam, phishing and fraudulent e-mails (Chart 21). Those considered most severe included malicious code, phishing, and spear-phishing (Chart 22). The threats were the same, with minor deviations, in all sectors monitored in 2019.

Over half the respondents identified **improvements in phishing, spear-phishing and fraudulent e-mails** as the major trend in the attacks against their organizations. Attackers demonstrated better knowledge of the environment and the language, making it harder to detect them.

Finding and paying cyber security experts has been a long-term issue for state administration and local government institutions. According to NÚKIB findings, the ministries and the Office of the Government lacked 153 cyber security employees in 2019. Nearly all respondents stated that salary conditions were the reason behind the cyber security vacancies in their organizations. Two thirds of the institutions dealt with the situation through outsourcing in 2019.

While the most severe attacks against state administration institutions remained the domain of state actors in 2019, local governments both in the Czech Republic and worldwide fell victim to cybercriminals in 2019. A ransomware attack against a region was reported to the Agency, with computers of the regional authority being infected.

Chart 21:

The most frequent attacks or attempted attacks against state administration and local government respondents in 2019 (%)

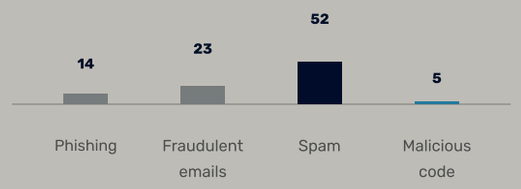
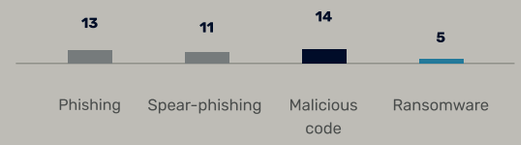


Chart 22:

The most severe attacks or attempted attacks against state administration and local government respondents in 2019 (%)



D | 02
Critical Infrastructure:
Limited Service Availability the Greatest Threat

According to the information available to the NÚKIB, no sophisticated and focused cyberattack targeting critical infrastructure (CI) information systems with serious consequences for the functioning of the state took place in the **Czech Republic** in 2019. Yet critical information infrastructure (CII) entities still faced hundreds to thousands of attempted cyberattacks. Up to half the detected cyber security incidents resulted in the **limited availability** of services which, for critical infrastructure entities, is the most essential aspect in terms of ensuring the smooth functioning of the state and society. A third of the respondents dealt with the most severe attacks in a matter of hours, but 9% addressed the consequences of some attacks for months (Chart 23).

Despite the general trend of dissatisfaction with the budget allocated to cyber security across other sectors, most respondents from the CI sector considered the 2019 budget sufficient. Compared to 2018, the budget increased at 45% of the respondents, while it remained the same for the same percentage of entities (Chart 24). This indicates that CI entities take cyber security seriously and invest the needed resources into security.

According to the CSA [xiii] critical information infrastructure (CII) means the communication and information systems of critical infrastructure (CI) elements. CI itself is defined by Act No 240/2000, on crisis management and on amendments to some laws (the "Crisis Act") [xiv], as an element or system of elements which, if disrupted, would have a serious impact on national security, the provision of the basic needs of the population, the health of individuals, or the national economy.

Typical CI elements include power plants, dams, airports, and telecommunications networks, but also strategic financial institutions and state authorities. If any of the elements is disabled, the provision of critical services (electricity, heat, water, pension payments) could be paralyzed or, in the worst-case scenario, physical damage could be caused (e.g. through cyber sabotage).

50% of CII incidents detected in 2019 resulted in limited service availability

Cyber Exercises as One Aspect of Critical Infrastructure Security

In 2019, the NÚKIB organized the first **"Electro Czech"** sector exercise for important obliged entities in electricity generation, transmission, and distribution. Approximately 40 participants from a total of 4 institutions went through a simulated complex crisis situation.

Chart 23:

The time needed for respondents to deal with the most serious incident in 2019 (%)

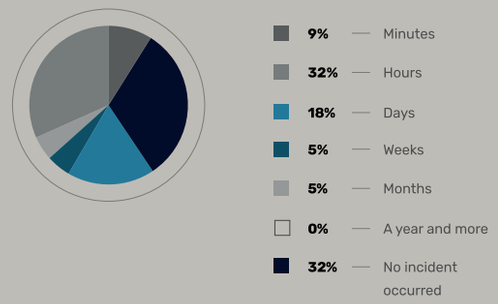
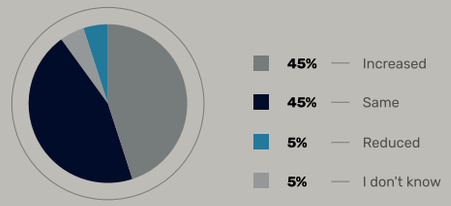


Chart 24:

How the budget allocated to CII respondent cyber security changed in 2019 (%)



D | 03

Financial Sector:

A Secured but Still very Tempting Target

As can be deduced from the absence of serious incidents in 2019, the **Czech banking sector is relatively well secured**. Nevertheless, there are still differences in the maturity of individual financial institutions, in particular in terms of protection against advanced cyber threats. In general, however, banks try not to underestimate cyber security because a compromise of their information systems could have far-reaching financial and reputational consequences. This translates in particular into investments in cyber security, inter alia in the form of higher salaries for experts. The financial sector was the only area where cyber security vacancies were not related to salary conditions. None of the responding financial institutions reduced its cyber security budget in 2019 and, on the contrary, 57% of them increased it (Chart 25). In addition to having cyber security experts, financial institutions tend to invest in user training as well. Over three quarters of the responding financial institutions actively test the resilience of their employees to cyber threats. Of all the responding organizations, financial institutions invest the most in cyber security.

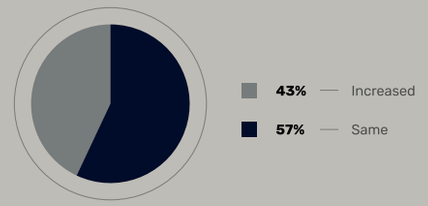
As in 2018, **the users themselves were the greatest vulnerability in the banking sector in 2019**. Attackers often exploited this long-term weak link, and many phishing campaigns were registered.

Attacks Tailored to Czech Users

Attacks on mobile internet banking systems are a continuing trend; **malicious applications directly targeting the clients of Czech banks emerged in 2019**. Malicious applications enable attackers to steal users' login details, for example the Word Translator translation application in Google Play for Android OS.[xv] Using this application, attackers tried to steal internet banking login details by recording user activity. Before it was blocked, Word Translator had more than ten thousand downloads. Half the malware detections were registered in the Czech Republic and approximately 40% in Poland. **Blockers Call 2019** was another similar application in Google Play, also targeting the users' internet banking systems.[xvi]

Graf 25:

How did financial institutions' cyber security budgets change in 2019 compared to the previous year? (%)



D | 04

Healthcare:

An Attractive and Inadequately Protected Target

In December 2019, there was a cyberattack against the systems of the Hospital of Rudolf and Stefanie Benešov, a referral for up to 400,000 people. Ransomware encrypted data on servers, hospital equipment and workstations. Standard treatment could not be performed at doctor's surgeries, planned operations were cancelled, and inpatients – including ICU patients – had to be transported to other nearby hospitals. It took almost a month for full recovery, while the consequences of the attack were estimated at CZK 40–50 million.

Greatest cyber security risks in the Czech healthcare system

- Inadequate regulation of cyber security standards
- Inadequate planning for crisis situations
- Obsolete software
- Risk of data theft

The funds allocated to cyber security by the responding organizations ranged between 0 and 5% of their budgets in 2019, and most respondents considered this inadequate. **Almost half the responding healthcare organizations would increase their cyber security budget by over 100%** (Chart 26), **which is more than any other responding sector.** Nevertheless, this fact is neither new nor surprising since cyber security has long been side-lined in hospitals as they have other budget priorities. In the light of the ransomware attacks against Czech hospitals in 2019 and early 2020, this situation needs to be changed to keep hospitals functioning.

As a result of the lack of funds, hospitals suffer from a shortage of cyber security experts. Almost half the respondents had 30–50% of their positions vacant (Chart 27), while for most of them the main reason was the salary conditions offered to job applicants.

Chart 26:

By what percentage should the hospital cyber security budget be increased, according to the respondents? (%)

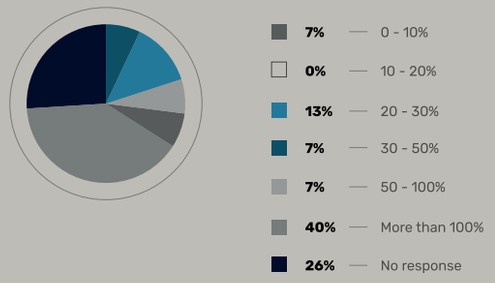
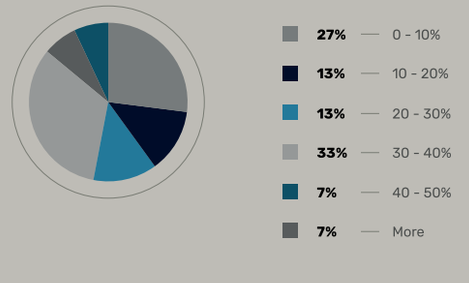


Chart 27:

Percentage of cyber security vacancies in hospitals in 2019 (%)



D | 05

Academia:
Increasing Interest from Cybercriminals

In 2019, academic institutions in the Czech Republic were targeted in particular by **financially motivated** cybercriminals. In that year, academia was a frequent target of spam, phishing campaigns and fraudulent e-mails, targeting both students and staff. The e-mails took various forms, from simple and widely distributed blackmailing to sophisticated and specifically targeted fraudulent e-mails in which the attackers posed as university staff.

As concerns phishing attacks in 2019, there was an evident continuing trend of increasing sophistication where, instead of using generic e-mails written with bad Czech grammar, the attackers demonstrated detailed knowledge of the environment at domestic universities. They pretended to be real university staff and the fraudulent websites referred to in the phishing and spear-phishing e-mails exactly replicated the visual style of those of the departments concerned. In one particular phishing attack, the attacker posed as the rector of the Czech University of Life Sciences and, in the e-mail, asked the addressees to submit a price offer using a template attached to the e-mail in the form of a malicious file.[xvii]

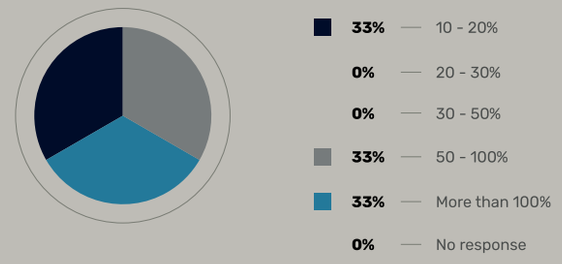
Universities are aware of the increased attention from cybercriminals. All respondents stated that their cyber security budgets had been increased. Yet at the same time, none of the respondents considered the funds sufficient, while two thirds of them would support an increase in funding by over 50% (Chart 28). In terms of ensuring cyber security, universities are specific in that they have to take into account furthermore not only staff and numerous departments but thousands of students, which entails corresponding costs.

Cyberattacks on educational and research institutions must not be underestimated. If university networks are compromised, **intellectual property and research results not yet published** may be leaked. If the attackers were to remain undetected for a longer period of time in the networks of **Czech universities**, this could undermine the competitiveness of the Czech Republic and result in losses of billions.

In the United States, schools and universities became one of the most common **ransomware** targets. In 2019, over 1,000 of them were attacked, making them the second most frequent target of this type of attack in the USA after towns. In 2019, indications of this trend were also noted in Europe, where the networks of the German Universität Giessen and the Dutch Universiteit Maastricht were infected by ransomware at the end of the year. There is a real possibility (probability of 25–50%) that Czech universities will become the targets of ransomware campaigns in 2020 and 2021.

Chart 28:

By what percentage should the university cyber security budget be increased according to the respondents? (%)



Chapter E
Measures

E | 01
National Cooperation in Cyber Security:
Implementation of Warnings and Cooperation with Other Supervisory Authorities

Monitoring of Key Entities and Methodological Support in 2019

In 2019, the NÚKIB carried out **15 inspections** according to the CSA and Decree No 82/2018, on cyber security (hereinafter the "CSD"). The inspections carried out with respect to obliged entities and entities subject to the CSA verify compliance with the obligations arising from the CSA and CSD. In the context of each inspection, approximately 150 inspection points are subject to verification.

In 2019, the NÚKIB provided **methodological support** based on a government resolution, covering all the ministries and the Office of the Government of the Czech Republic. The Office of the Chamber of Deputies and the Chancellery of the Senate of the Parliament of the Czech Republic, as well as the Office of the President of the Czech Republic, also join in the methodological support on a voluntary basis every year. The methodological support is based on an individual cyber security analysis of the entities and on analysis-based consultations regarding appropriate solutions to the cyber security deficiencies identified. The support covers systems administered by the entities concerned which can be accessed by employees from an external network (the internet).

The Warning About Huawei and ZTE Technology and Software is Still Applicable

At the end of 2018, the NÚKIB issued a warning regarding the use of technology and software from Huawei Technologies and ZTE Corporation based in the People's Republic of China. The warning was still applicable in 2019 and has been gradually acted on.

In the course of 2019, the NÚKIB carried out a survey among the obliged entities under the CSA, which showed that 27 obliged entities were using Huawei and ZTE technologies in their critical information infrastructure (CII) systems, important information systems (IIS) and basic service providers (BSP) at the time of the survey. After carrying out a risk analysis based on the warning, 22 of the obliged entities removed the technologies of the aforementioned companies from their CII, IIS and BSP information systems.

Cooperation with Other Supervisory Authorities in Monitoring in 2019

In the field of monitoring, the NÚKIB has a long-standing commitment to **cooperating with other supervisory authorities** (regulators) and ensuring maximum joint harmonization in the areas supervised (regulated) by the regulators which overlap with cyber security. In addition to the Czech National Bank and Civil Aviation Authority, which have been cooperating with the NÚKIB on a long-term basis, cooperation was established in 2019 for example with the **State Office for Nuclear Safety** and the **Czech Telecommunication Office**. This cooperation aims in particular at minimizing the burden on regulated authorities and entities. In addition to the monitoring, the identification of information systems falling within the scope of the CSA continued.

CONTENTS

Number of Designated Entities at the End of 2019:

47 administrators and operators of critical information infrastructure information and communication systems	**109** critical information infrastructure information and communication systems
70 administrators and operators of important information systems	**178** important information systems
38 administrators and operators of basic service information systems	**42** basic service information systems

NÚKIB Support Materials on the Internet

The NÚKIB regularly publishes support materials and schematics concerning the interpretation of the Cyber Security Act to simplify cyber security issues for the professional and general public on its website. In 2019, for example, the NÚKIB updated its methodological materials on public procurement in ICT, cyber security, and other important documents.

The support materials are available at: **https://www.govcert.cz/cs/regulace-a-kontrola/podpurnematerialy/.**

E | 02
Cyber Security Exercises:
An Increase in Interest and the Number of Exercises Performed

In 2019, the NÚKIB registered a significant increase in demand for exercises from organizations active in the Czech Republic. The trend was, to a lesser extent, already discernible in the previous year, yet it was 2019 that became a real turning point in terms of demand for exercises. On the basis of these changes, one can conclude that the exercises are becoming a respected tool for improving cyber security. **Senior officials at the participating institutions from the state**

administration and energy sectors, as well as experts on the subject, **supported and actively participated in the exercises.** The increased interest was reflected in the number of exercises. In 2019, the number of exercises organized by the NÚKIB rose by 42% while the number of participants rose by 27% year-on-year (Charts 29 and 30). **Important exercises focused on law enforcement authorities, state administration and the energy sector were undertaken in 2019.**

Why are Cyber Exercises Useful?

Exercises are an invaluable **source of new knowledge, experience, and technical skills.** They provide the NÚKIB with an **opportunity to identify and point out weaknesses** in cyber security, and they are also an excellent **tool to verify and review policies and processes**. Finally, the exercises help to **identify, define, and confirm specific trends in the field** and the outputs represent valuable knowledge that can be used to **prepare further public awareness-raising and educational activities.** The demand and responses from foreign partners, such as the United States, Israel and Taiwan, confirm that the exercises have made a **major contribution to Czech foreign policy.**

Chart 29:

The number of exercises organized by the NÚKIB in 2018 and 2019

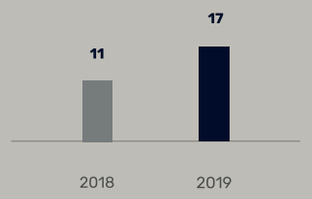
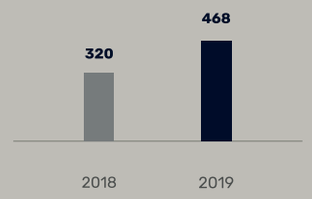


Chart 30:

The number of participants in the exercises organized by the NÚKIB in 2018 and 2019



Cyber Security Exercises in 2019

17
Number of exercises organized by the NÚKIB

12
Number of domestic exercises

3
Number of exercises for foreign partners

3
Number of multinational exercises in which the NÚKIB participated

468 (from 90 countries)
Number of participants in exercises organized by the NÚKIB

276
Number of participants in the Czech Republic

192
Number of participants abroad

Significant knowledge gained from the exercises in 2019:

01

To ensure timely, effective, and adequate reaction to serious cyber incidents, organizations should have pre-prepared cyber security emergency plans and the relevant employees should be familiar with such plans.

02

One of the greatest cyber security challenges is to share information among partners (both domestic and foreign) essential to place cyberattacks within a wider context, to uncover all the attackers' activities, motivations and goals, and to adopt adequate measures.

NÚKIB Achievements in International Exercises in 2019

In April 2019, the Czech team formed by the NÚKIB and experts from the state, private and academic spheres placed second (among 22 teams) in the "Locked Shields" international exercise, considered the world's most complex technical exercise.

In November, the Czech team, including NÚKIB employees, won the "CODE 2019" international exercise held in Taiwan.

E|03

Awareness-raising and Education in the Czech Republic:
Educating Users of All Ages

Education is an especially important variable in cyber security in the Czech Republic. The safe use of digital technologies is one of the basic digital literacy competences, and deserves appropriate attention. Awareness-raising activities in cyber security were quite varied in the Czech Republic in 2019 and, in addition to public officials, they focused primarily on vulnerable population groups, i.e. in particular children and senior citizens.

The nation-wide cyber security awareness-raising and educational activities carried out in 2019 included, for example:

E-Security (E-Bezpečí):
A Palacký University Olomouc internet security project focused on various target groups (senior citizens, teachers, parents, pupils, and students).

Smart School (Chytrá škola):
A portal providing information mainly to teachers and parents.

Safely on the Internet (Internetem bezpečně)
A project of the "you connected, z.s." association, under which an information website, awareness-raising videos, lectures, and educational textbooks were prepared.

Be Safe Online (Buď safe online):

An awareness-raising online project from Avast, an antivirus company, which provides materials and interactive games for teachers, parents, and children. In cooperation with YouTuber Jirka Král, a set of educational videos was prepared focusing on cyberspace threats.

Cyber Compass: (Kyberkompas)

A six-part online course from Masaryk University provided to both the university students and the general public. The course improves user skills in equipment security, password use, and incident reporting.

Safely on the Net (Bezpečně na netu):

An awareness-raising project from CZ.NIC, under which mainly audio-visual awareness-raising content is prepared. The project offers many short educational films and the #Martyisdead eight-episode series.

The NÚKIB updated its e-learning portal and online courses in 2019. For a large group of public officials, the NÚKIB updated the **Master Cyberspace! ("Dávej kyber!")** course focused on the basics of cyber hygiene and information security. A total of 6,953 users enrolled in the course, and **5,172** obtained the completion certificate. This number was added to the **21,443** already trained civil servants from 2018.

The other NÚKIB online course, **Control Cyberspace! ("Šéfuj kyber!")**, is by contrast designed for IT administrators, people in cyber security management positions, and other positions subject to the CSA. 422 users enrolled in the course and **287** obtained the completion certificate.

In the field of cyber security awareness-raising and educational activities, the NÚKIB furthermore pursued the following projects:

Little Cybertown

In 2019, the NÚKIB started preparing an innovative **board game for kindergartens, called Little Cybertown (Městečko kybernetov)**, which presents, in a natural way, the problems of addiction to communication technologies, cyberbullying, cybergrooming, and health to children aged between 5 and 9.

Digital Trace

In 2019, the online **Digital Trace (Digitální stopa)** educational activity was amended and improved. This is an entertaining interactive story for fifth and sixth graders which shows, in a playful way, the current risks, and teaches safe behaviour on the internet.

Sensational Seniors

In cooperation with the **Sensational Seniors (Senzační senioři, SenSen)** association, the NÚKIB took part in a series of 7 lectures for senior citizens held in towns across the Czech Republic. The series ended with a conference in Prague.

Vanda and Eda in the Online World

The NÚKIB prepared a book for kindergartens called **Vanda and Eda in the Online World (Vanda a Eda v Onl@jn světě)**, which includes methodological cards to be used by teachers. The book contains stories which educate preschool children about risks associated with digital technologies in a simple way. The NÚKIB published the book in print form, distributed it to over 5,300 kindergartens in the Czech Republic, and offers the book for download on its website. [xviii]

Network Security Monitoring Cluster

In 2019, the NÚKIB continued to support the **Network Security Monitoring Cluster** project for the development of regional secondary school **junior cyber security excellence centres** to provide expert and technical assistance in cyber security education throughout the region. The goal is to have at least one secondary school in every region acting as a junior centre.

In 2019, the NÚKIB engaged in working groups of the Ministry of Education preparing revisions of the framework education programs. It also commenced cooperation with the Ministry of the Interior Committee for Educational Activity Accreditation, in the context of which the NÚKIB gives opinions on accreditation applications relating to cyber security. The NÚKIB delivered a total of 5 opinions in 2019.

Research and Development: Cryptography and Protection from Harmful Radiation

In 2019, the NÚKIB worked on several research and development projects in applied cryptography, the development of special measuring methods and technologies to ensure protection from harmful radiation, and cryptographic means to protect confidential information.

15	lectures for state administration, libraries, universities, courts, hospitals etc.	**17**	activities for kindergarten and primary school pupils	**8**	lectures for secondary school students
8	lectures for senior citizens	**6**	lectures for parents		

E|04

International Cooperation:
Contribution to Global Cyber Security

Many decisions essential for the development of cyber security in the Czech Republic are made at both national and international levels. The cyber security interests of the Czech Republic are represented in key international organizations, in particular the EU, UN, and NATO, as well as the OECD and OSCE, are represented by the NÚKIB jointly with the Ministry of Foreign Affairs (hereinafter the "MFA"), the Ministry of Defence, and other partners[6]. In 2019, the NÚKIB focused in particular on negotiations with EU member states and institutions, mainly with respect to the agenda of the so-called cyber security package (e.g. the ECCG – European Cybersecurity Certification Group), the EU Toolbox for 5G Security, the conclusions of the European Council and the Council of the European Union (Cyber Diplomacy Toolbox, Blueprint), obligations arising from the NIS Directive, and the new legislative proposal for a competence centre. The so-called Open Working Group was set up at the UN, with both the NÚKIB and the MFA actively contributing to its activities.

Prague 5G Security Conference and Publication of the Prague Proposals

In 2019, the NÚKIB and the MFA together organized the first international expert conference on 5G network security. Prague 5G Security Conference was held on 2 and 3 May 2019 under the auspices of Andrej Babiš, Prime Minister of the

[6] Ministry of Industry and Trade, Czech Telecommunication Office etc.

Czech Republic, and Tomáš Petříček, Foreign Minister of the Czech Republic, who attended the conference in person as well. The two-day closed international conference was attended by over 150 government officials and experts from over 32 states, including EU and NATO representatives.

The main output of the expert conference was the publication of the so-called Prague Proposals, a series of recommendations on 5G network security. The Prague Proposals emphasize, inter alia, the **importance of the non-technological aspects** of communication infrastructure security and the crucial role of users' (and the state's) confidence in the producer of the hardware and software used.

The Prague 5G Security Conference and the Prague Proposals themselves attracted a large international response and became the guideline for many bilateral cyber security agreements signed in 2019. Nontechnological aspects and the issue of confidence in the supplier were also included among the key 5G network security characteristics and reflected in the EU Toolbox for 5G Security. Hence, the Prague Proposals represent a significant contribution by the Czech Republic to the formulation of 5G security principles at global level, to be followed by a second Prague 5G Security Conference planned for May 2020.

The Prague Proposals:

A translation of the Prague Proposals is available at:
https://nukib.cz/download/5G%20site/Prazske-navrhy-5G-Sec-190503-cz.pdf.

The original is available at:
https://nukib.cz/download/5G%20site/Prague-Proposals-5G-Sec-190503.pdf.

EU Toolbox: Measures for the Security of 5G Networks in the EU

The toolbox is a set of specific measures on how the security of 5G networks in member states should be set, regulated, and implemented. The Czech Republic, together with France and other member states, had a leading role in the preparation of the EU Toolbox for 5G Security, which also meant that the Czech approach was largely reflected in the final document. Concerning the most important aspects, one can mention the requirement for risk analyses to include an assessment of both technological and non-technological threats. One example is the legal and political environment of the producer's country of origin, since this has a major impact on the credibility of the technologies produced.

E | 05
Network Probes in Key State Authorities:
New Partners and New Projects

In order to raise awareness of harmful activities across strategic state networks in the Czech Republic, the NÚKIB has been implementing a project called **"System for the Detection of Cyber Security Incidents in Selected PAIS"[7].** This aims to make it easier for the administrators of key state networks to detect potential attackers and provide better network protection by deploying network probes.[8]

In the context of this system, the **capacities of the central analytical tool** were improved in 2019. The tool was linked to the NÚKIB's internal databases, and proposals for changes to the link are under preparation so subsequent operation and experience can provide other necessary functionalities and other types of data. In addition, rules were specified for

[7] Public administration information systems.
[8] The project is unrelated to the plans for probe deployment in electronic communication networks by Military Intelligence.

the automated searching of suspicious data traffic and events targeting multiple organizations involved.

In the course of the year, negotiations were initiated with other prospective partners who operate their own network probes monitoring network perimeter traffic. Agreements with the partners regarding their engagement in the project were specified, and the technical connection itself was performed at the end of the year.

At the end of 2019, network probes were deployed by 23 government partners. Local administrators were properly trained and started sharing with GovCERT.CZ cyber security incidents and selected data about network traffic passing through the network perimeter.

Network probes help warn about suspicious data connections and anomalous data volumes leaving a particular network, detect "checking out" the network from the outside, and serve as an early warning tool for impeding attacks. Probes can also retrieve and store descriptive traffic data to create an audit trail for later examination of what has happened at a given ministry or office. Thanks to data sharing with partners, the NÚKIB will be able to trace security incidents that would not otherwise be detected by a ministry or assessed as dangerous, and inform other organizations before they are hit by an attack.

Chapter F

Outlook for Cyber Security Trends for 2020 and 2021

Ransomware:

Cybercriminal activities using malware which blocks access to data and demands ransom will almost certainly (probability 90–100%) be one of the major threats in 2020 and 2021. Although the number of infected users might continuously decrease, a ransomware campaign trend of greater sophistication and targeting can already be observed and is highly likely to continue in 2020 and 2021. As with phishing, the attackers exploit the covid-19 pandemic to increase the success rate of their attacks. In the light of foreign trends and the development so far in the Czech Republic, it is highly likely (probability of 75–85%) that local government institutions and healthcare and educational establishments, in particular colleges and universities, will become ransomware targets.

Cloud:

Organizations have been increasingly using cloud infrastructure and platforms as a service, which in addition to many positives, carries its own risks. This use means that organizations' sensitive data are located in an environment, the maintenance and monitoring of which is not under their control and which is accessible from the internet. Moreover, cloud infrastructure is often inappropriately configured. Trade secrets and other sensitive data residing in a cloud are an attractive target for both foreign state actors and cybercriminal groups. A trend of increased cloud service compromise risk is highly likely (probability of 75–85%) in 2020 and 2021 and, in particular, the service providers will become the targets. It cannot be ruled out (probability of 25–50%) that Czech institutions or companies will be among those impacted.

Mobile malware:

In 2020 and 2021, Czech users are likely (probability of 55–70%) to more frequently encounter malicious mobile applications that pose as legitimate ones. Attackers are highly likely (probability of 75–85%) to be primarily seeking access to their victims' internet banking systems.

Phishing, spear-phishing and fraudulent e-mails:

2019 witnessed a trend of more sophisticated and targeted malicious e-mails in which attackers demonstrated better knowledge of the environment, language, and used highly varied topics. This improvement in social engineering techniques will almost certainly (probability of 90–100%) continue in 2020 and 2021. A trend of exploiting the covid-19 epidemic in aggressive phishing campaigns is already evident in the Czech Republic and around the world at the beginning of 2020. It cannot be ruled out (probability of 25–50%) that Czech users will more frequently encounter not only fraudulent e-mails but also fraudulent phone calls using deepfake technologies which enable the attackers to imitate the voice of a stranger (e.g. a company director). This method can be used for highly sophisticated spear-phishing campaigns as well.

Lack of experts:

In 2019, some sectors faced the problem of how to fill cyber security vacancies with experts, usually due to insufficient funds. This situation is highly likely (probability of 75–85%) to continue in the Czech Republic in 2020 and 2021. Cyber security requires significant investments and is often side-lined in many organizations due to the prioritization of other areas. In combination with the annually growing number and improvement of cyberattacks, the situation is likely (probability of 55– 70%) to result in a higher number of successful cyberattacks in the selected sectors (healthcare, education, state administration, and local government institutions) in 2020 and 2021.

Chapter G

Annexes

G | 01

Annex 1:

Details of Incidents Handled by GovCERT.CZ

Over 2019, GovCERT.CZ employees received a total of 217 relevant cyber security incident reports from Czech and foreign partners. The reports were assessed in terms of the areas of competence of the GovCERT.CZ team and then processed either using its own resources or by forwarding them to the competent authorities. In the past year, 78 cyber security incidents falling within the area of competence of Government CERT were assessed, processed, and handled on the basis of the reports received and information it gathered itself.

This is a noticeable increase compared to 2018, when 164 incidents were reported to GovCERT.CZ and 54 incidents were resolved.

The most serious incidents handled by GovCERT.CZ in 2019 indisputably included the case of the infection of the systems of the Hospital of Rudolf and Stefanie Benešov and the OKD mining company with Ryuk ransomware. Although neither the Benešov hospital nor OKD are obliged entities under the CSA, the NÚKIB, in agreement with the impacted organizations, sent its team to the site. The team members participated in the recovery of the information network, forensic and network analysis, and assistance in setting up basic security features.

Another incident handled by GovCERT.CZ in 2019 was the infection of a state institution with Emotet malware. The institution delivered disks from ten infected computers for analysis, on the basis of which the Agency made recommendations for handling the infection.

Chart 31: Incidents handled in 2018 and 2019 by month

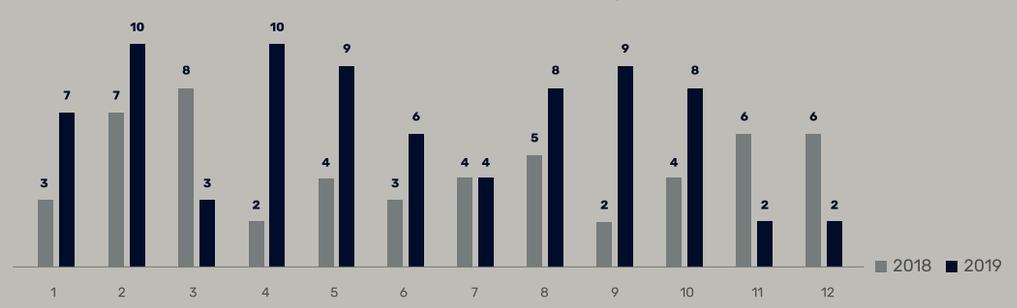


Chart 32: Incoming incident reports in 2018 and 2019 by month

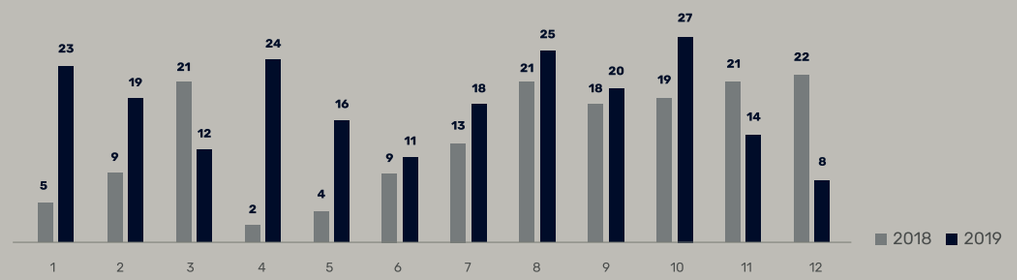
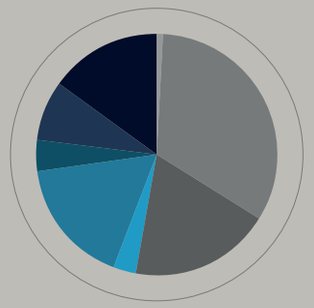


Chart 33:

Classification of incidents handled in 2019



The description of categories is based on the incident reporting form:

- **15%** — Malicious content (e.g. virus, worm, trojan horse, dialer, spyware)
- **8%** — Penetration (e.g. successful compromise of an application or user account)
- **4%** — Attempt to penetrate a system (e.g. attempt to exploit a vulnerability, compromise an asset, "0-day" attack)
- **17%** — Information security breach
- **3%** — Gathering of information (e.g. scanning, sniffing, social engineering)
- **19%** — Fraud (Phishing)
- **33%** — Availability
- **1%** — Offensive content (e.g. spam, cyberbullying, inappropriate content)
- **0%** — Administrative (e.g. security incident caused by clerical error)

G | 02

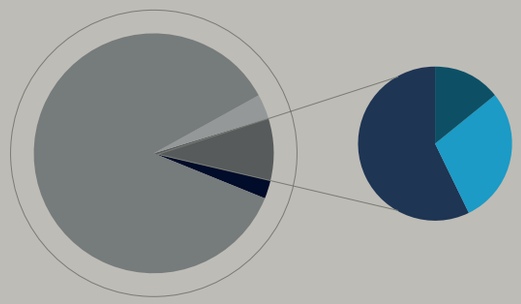
Annex 2:

Implementation of the Action Plan

2019 was the penultimate year of the implementation of the existing Action Plan on the National Cyber Security Strategy of the Czech Republic for the period from 2015 to 2020. This resulted in a decreasing absolute number of tasks assigned compared to previous years. In addition, uncompleted tasks from prior years were completed in 2019. It can be said that most of the tasks were completed or being completed on an ongoing basis, and only a few tasks were completed partially, i.e. with some deficiencies. **The tasks completed** (in cooperation with other entities) in 2019 included, for example, the drawing up of a national plan for cyber security research and development, and the creation of a database of cyber security research projects from which information is provided to other entities.

Chart 34:

Implementation of the Action Plan in 2019



- **73** — Being completed
- **7** → **1** — Being completed – from prior years
- **3** — Being completed partially
- **2** — Being completed partially – from prior years
- **2** — Completed
- **4** — Completed partially – from prior years

One example of a task **being partially completed** was the creation and introduction of a honeypot system for the detection of cyber threats and anomalies in network traffic to identify potential cyber threats. The task was completed only partially in 2019. Honeypot detectors are currently deployed in NÚKIB networks, and their number is being gradually increased. Central analytical software, to which selected partners are connected, is used to detect anomalies in network traffic. New partners are currently being connected depending on the available analytical software license capacity, and the system is being optimized and further extended.

G | 03

Probability Expressions Used in the Report on the State of Cyber Security in the Czech Republic in 2019

Probability expressions and their percentage values.

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

G | 04

Sources:

i **Rozhlas. 2020. Na nemocnici v Benešově útočil ruský virus Ryuk. Jermanová odmítá, že by někdo požadoval výkupné.** https://www.irozhlas.cz/zpravy-domov/nemocnice-benesov-kyberneticky-utok-ransomware-vykupne-ochrana-osobnich-udaju_2001140615_cha

ii **Policie ČR. 2018. Kyberkriminalita.** https://www.policie.cz/clanek/kyberkriminalita.aspx

iii **BIS. 2018. Výroční zpráva Bezpečnostní informační služby za rok 2017.** https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2017-vz-cz.pdf

iv **401TRG. 2018. Burning Umbrella: An Intelligence Report on the Winnti Umbrella and Associated** State-Sponsored Attackers. https://401trg.com/burning-umbrella/

v **Reuters. 2019. BASF, Siemens, Henkel, Roche target of cyber attacks.** https://www.reuters.com/article/us-germany-cyber/basf-siemens-henkel-roche-target-of-cyber-attacks-idUSKCN1UJ147

vi **Cyberscoop. 2017. Research claims CCLeaner attack carried out by Chinese-linked group.** https://www.cyberscoop.com/ccleaner-attack-china-intezer-labs-piriform-apt17/

vii **Check Point. 2019. October 2019's Most Wanted Malware: the Decline of Cryptominers Continues, as Emotet Botnet Expands Rapidly.** https://blog.checkpoint.com/2019/11/12/october-2019s-most-wanted-malware-the-decline-of-cryptominers-continues-as-emotet-botnet-expands-rapidly/

viii **Check Point. 2020. Helping you navigate the ever-changing security landscape: Check Point Research's 2020 Cyber Security Annual Report** https://blog.checkpoint.com/2020/01/15/the-2020-check-point-cyber-security-annual-report-is-available/

ix **BIS. 2019. BIS spolupracovala se společností Avast na odvrácení útoku na její produkty.** https://www.bis.cz/aktuality/bis-spolupracovala-se-spolecnosti-avast-na-odvraceni-utoku-na-jeji-produkty-6acda7bf.html

x **CyberScoop. 2017. Research claims CCLeaner attack carried out by Chinese-linked group.** https://www.cyberscoop.com/ccleaner-attack-china-intezer-labs-piriform-apt17/

xi **Econlab. 2019. Analýza: Necenová kritéria při zadávání veřejných zakázek v EU.** https://econlab.cz/files/2019/07/2019-07-22-MPSV%20-%20studie%20kriteria.pdf

xii **ÚOHS. 2019. Č. j.: ÚOHS-S0262/2019/VZ-30266/2019/523/Jma.** https://www.uohs.cz/cs/verejne-zakazky/sbirky-rozhodnuti/detail-16400.html

xiii **Národní centrum kybernetické bezpečnosti. 2018. Aktuální legislativa.** https://www.govcert.cz/cs/regulace-a-kontrola/legislativa/

xiv **Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), v aktuálním znění.** https://www.zakonyprolidi.cz/cs/2000-240

xv **Eset. 2019. ESET informuje o další nebezpečné aplikaci, nástroj pro překládání textů cílil na klienty bank v Česku.** https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-informuje-o-dalsi-nebezpecne-aplikaci-nastroj-pro-prekladani-textu-cilil-na-klienty-bank-v-ces/

xvi **Česká spořitelna. 2019. Upozornění na podvodnou mobilní nebankovní aplikaci.** https://www.csas.cz/cs/zpravy-z-banky/2019/01/22/upozorneni-na-podvodnou-mobilni-aplikaci

xvii **Česká zemědělská univerzita. 2019. Cenová poptávka.** https://www.oikt.czu.cz/cs/r-13742-spam/r-13743-vzory/cenova-poptavka-ceska-zemedelska-univerzita-v-praze-uni-784-.html

xviii **NÚKIB. 2019. Vanda a Eda v Onl@jn světě.** https://nukib.cz/download/vzdelavani/rozcestniky/Vanda_a_Eda_v_Onljn_svete_kniha_s_kartami.pdf