NÚKIB

Report on the state of cyber security in the Czech Republic in 2018

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Summary by the NÚKIB Director

Ing. Dušan Navrátil

NÚKIB Director

The National Cyber and Information Security Agency (hereinafter the "NÚKIB" or the "Agency") is submitting a new version of the Report on the State of Cyber Security in the Czech Republic for 2018. In this report, we assess the current cyber security situation in our country, look back at the recent past, highlight the greatest threats and targets of attackers, and the effects successful cyber attacks can have.

Cyber security is a society-wide issue today and therefore a wide range of relevant actors have been involved in the drafting of this report. Besides the NÚKIB, public administration bodies, critical infrastructure managers, the academic sphere, security experts and prominent private cyber security companies have contributed to its creation. I would like to thank all of them for their help. Thanks to their materials, comments and observations, the picture of the status of cyber security is more accurate and will allow us to progress a little further in the protection of cyberspace. The report has been prepared using three main sources – information available to GovCERT.CZ, which is operated by the NÚKIB, information obtained from the Agency's partners, and open sources.

The number of cyber threats the Czech Republic faces is increasing. The number of cyber attacks and their sophistication is on the rise, attackers are coming up with new methods of attack and, at the same time, the possible attack field is constantly expanding, partly due, for example, to the rise of Internet of Things (IoT) devices.

From the perspective of the state, the most important cyber threat actors in terms of available human, financial and time resources are **state actors**. Their primary goal is to gather strategic information through espionage operations in cyberspace and then use it to their advantage. In the case of the Czech Republic, according to the information available to the NÚKIB, this specifically means operations of actors linked to the Russian Federation and the People's Republic of China. The second most important actor in cyberspace threats are people

and organizations involved in criminal activities. As **cybercrime** is profitable and ever easier to get involved in, it will continue to pose a threat to organizations and individuals in the years to come.

Regarding the means of attack, in 2018, both internationally and in the Czech Republic, extortion attacks (ransomware) became less prevalent and were replaced by **cryptocurrency mining through malware**. This trend suggests the latter is likely to be a more effective tool to generate financial gain than ransomware attacks. Despite the impact on the computational performance of the infrastructure of the attacked entities, the illegitimate extraction of cryptocurrencies is a minor threat from the perspective of ICT protection. Unlike ransomware attacks, it is not destructive and does not compromise the availability of important data.

Another trend was the **increasing number and sophistication of targeted spear-phishing attacks,** showing that offenders often have excellent knowledge of the environment and invest a lot of time in preparation. Financial institutions and their clients are frequent targets of spear-phishing attacks in the Czech Republic, but in recent years attacks against Czech universities have also increased. The main motivation of the attackers is direct financial gain, but efforts to steal intellectual property are not an exception. Cyber attacks on educational and research institutions should not be underestimated. In the case of compromises of university networks, **intellectual property and research results** not yet published may be **leaked**. If attackers in the networks of Czech universities were to remain undetected for a longer period of time, the result could be a **significant weakening of the Czech economy's competitiveness.**

Energy and banking are key sectors for which cyber security is crucial. A trend worth paying attention to in the energy sector is the deployment of **SMART meters**. These represent both a way of optimizing energy flows and a potential vulnerability for attackers wanting to interrupt the power supply. The manufacturers of deployed IoT technologies should thus ensure they are adequately secured so that the risk of cyber attack is minimized. As far as banking is concerned, the issue is mainly **attacks on mobile internet banking applications**. More and more people use mobile apps to manage their finances, and hackers have quickly adapted to this. The modified QRecorder application that damaged Czech bank clients was an example of this trend in 2018.

A **shortage of cyber security experts** is a major problem across both the public and the private sectors. This was stated by 40% of the 42 institutions that provided the NÚKIB with information for this report. As a result, some basic security processes may be delayed, or the staff on which the institution's cyber security depends may be overworked. A specific risk factor in the Czech Republic is the **application of the Public Procurement Act**, where procurement procedures with price as the main or sole criterion prevail. Potentially risky components can enter strategically important systems due to this insistence on the lowest price offer. At present, the law allows for criteria other than price to be considered, but the use of these criteria requires, in many cases, greater capacity on the part of the contracting authority and increases the risk of a possible review which may disproportionately extend the tender procedure.

One of the ways the NÚKIB can respond to cyber security threats is by issuing **warnings**. The NÚKIB issues such warnings when it becomes aware of a cyber threat that needs an immediate response. On 17 December 2018 the NÚKIB warned against the use of technical and software resources by Huawei Technologies Co., Ltd. and ZTE Corporation. This was substantiated by a combination of knowledge and findings obtained during the exercise of the Agency's powers. The NÚKIB also issued a supporting methodology for this warning which specifies the measures that the administrators of information and communication systems covered by the Cyber Security Act can adopt.

Cyber security exercises are ways cyber security can regularly be improved. Their results have long shown that ignorance of the functioning of cyberspace, potential risks and the principles of digital hygiene often leads to inconsistent compliance. It is therefore necessary to raise awareness among cyber security staff, including middle and senior management. One consequence of this situation is, inter alia, that for several years the **user** has been the most common entry point for obtaining information and data available in internal networks of organizations. Attackers target the user as the weakest link in cyber security by using social engineering techniques,

the nature of which remains unchanged but whose number and sophistication is increasing.

There are many educational projects in the Czech Republic, but **increasing digital literacy** and resilience to threats across society is a long-term process that will require constant work. The NÚKIB is therefore involved in working groups preparing revisions of framework educational programs. In particular, the Agency strives for more significant integration of cyber security issues into school education. These efforts have yielded significant results and cyber security is penetrating into education as an integral part of digital literacy.

The education of people working for the state and public administration is also a priority, as they come into contact with sensitive data in the exercise of their professions. The NÚKIB has therefore launched two **on-line courses for public administration** that were successfully completed by more than 21,500 civil servants by the end of 2018.

To make the Czech Republic better aware of harmful activities in the strategic networks of the state, the NÚKIB has implemented a project focused on a system for detecting cyber security events in public administration information systems. Its aim is to provide better protection of key government networks through the **deployment of network probes.** Thanks to data sharing with partners, the Agency will be able to trace security incidents that would not be detected in a department or would not be evaluated as dangerous, and to inform other organizations about them before they are attacked. At the end of 2018, network probes had been deployed with 20 partners from state administration.

Cyber security is often seen as a phenomenon that can only be dealt with by technical experts. It is necessary to move away from such an understanding for it to be effectively provided. **Cyber security is necessary throughout public, working and, to some extent, private life** – it is part of national security, foreign policy, the economy, education and our daily lives. The involvement of management in all government institutions is essential to increase cyber security in the country and to manage crisis situations.

We do not expect cyber threats to slow down in the coming years. Attackers will look for new ways to break protection, and it is up to us all to confront them – not just to respond to attacks that have already taken place, but to anticipate them and be prepared for them before they occur. The cyber security of our country will never be absolute, but it is our duty to get as close to this situation as possible.

Contents

2018

Cyber security in the Czech Republic in figures

164

CYBER INCIDENTS REPORTED TO GOVCERT.CZ

54

REPORTED CYBER INCIDENTS RESOLVED ON GOVCERT.CZ

1 079

SECURITY INCIDENTS HANDLED BY CSIRT.CZ – - THE NATIONAL SECURITY TEAM OF THE CZECH REPUBLIC

6 815

CRIMES IN THE FIELD OF CYBERCRIME AND INTERNET CRIMES

518

PHISHING ATTACKS REPORTED TO CSIRT.CZ

10

UNIVERSITIES EXPOSED TO A WAVE OF PHISHING ATTACKS

11

CYBER SECURITY EXERCISES CONDUCTED BY NÚKIB

77

COUNTRIES PARTICIPATING IN THE EXERCISES

320

PARTICIPANTS IN CYBER SECURITY EXERCISES ORGANIZED BY NÚKIB

21 443

TRAINED STATE ADMINISTRATION SERVANTS

178

IMPORTANT INFORMATION SYSTEMS

30

BASIC SERVICE OPERATORS

45

CRITICAL INFORMATION INFRASTRUCTURE ENTITIES

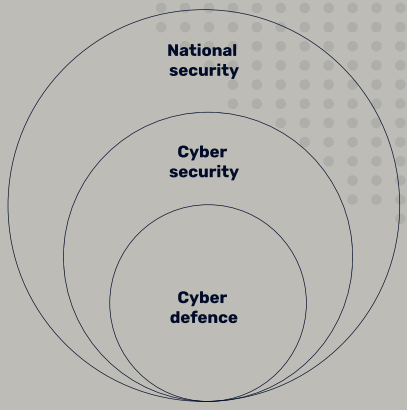
What is cyber security and how is it solved in the Czech Republic?[i]

Three categories that define cyber security:

A	B	C
Prevention	**People**	**Confidentiality**
Detection	**Processes**	**Integrity**
Reaction	**Technologies**	**Availability**

Czech Republic

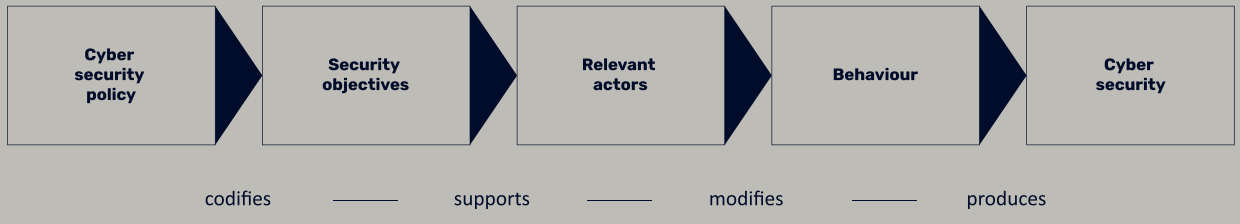
The coordinator in the field of cyber security of the Czech Republic is the National Cyber and Information Security Agency, which is the central administrative body for cyber security, including the protection of classified information in the area of information and communication systems and cryptographic protection. He is also responsible for non-public service within the Galileo satellite system. The NCISA was established on 1 August 2017 on the basis of Act No. 2015/2017 Coll., Amending Act No. 181/2014 Coll., On cyber security and amending related laws. It became the National Cyber Security Center which operated previously under the National Security Authority (NSA).



The role of the state in ensuring cyber security

- Cyber defence
- Critical information infrastructure protection
- Cybercrime
- Operation of intelligence services

The tension between functionality and security requirements is reflected through cyber security policy.



Actors

Many actors with different interests operate in cyberspace. These include states and their sponsored hacking groups, cybercriminals, terrorists, hacktivists, hackers using their skills for their own benefit (black hats) and inexperienced individuals (script kiddies). On the other hand, there are also ethical hackers trying to discover and warn of vulnerabilities to prevent their abuse.

It is also possible to distinguish between external attackers and 'insiders'. An insider may be a dissatisfied employee who, for example, collects sensitive or classified information to pass it on to foreign actors, sell it or publish it to harm their employer.

According to the information available to the NÚKIB, the greatest threats to the **Czech Republic** are foreign powers and cybercriminals. However, for the sake of completeness this report also includes links to other groups.

State actors and state-sponsored groups:

State-sponsored actors have long been the most significant threat from the perspective of the state. In general, they have the human, financial and time resources to make their cyberspace operations technically sophisticated and persistent. They primarily seek strategically and politically important information and to obtain military benefits for possible future conflicts. At present, the operations of actors linked to the Russian Federation and the People's Republic of China pose a particular threat to the **Czech Republic**.

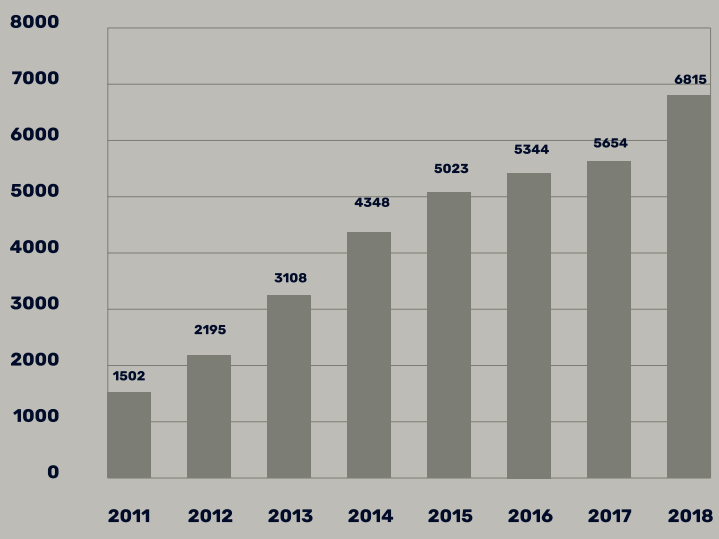
Cybercriminals:

The main motivation of cybercriminals is financial gain, which is also reflected in the techniques they use. Their arsenal often involves various types of ransomware, social engineering to infiltrate their victims' bank accounts, and fraudulent e-mails to lure money out of people. While a few years ago cybercrime was largely in the hands of technically proficient hackers, in today's cyber environment anyone who is able to pay can get the hacking tools needed. Custom hacking, or "Malware-as-a-Service", has become one of the frequently sought commodities on the darknet and an increasing number of attacks have been carried out with tools purchased there. As cybercrime is profitable and easier to get involved in, it will continue to pose a threat to organizations and individuals in the years to come.

According to statistics from the Police of the Czech Republic, cybercrime and Internet crime are on the rise and the number of

Graph 1:

Cybercrime cases investigated in the Czech Republic between 2011 and 2018



Source: policie.cz

[1] *The Darknet is a hidden part of the Internet that can be accessed using special software.*

cases is increasing every year **in the Czech Republic.** [ii]

Terrorists:

Terrorists are not currently a major threat to the cyber security of the **Czech Republic**. Islamic State has gained much attention through its activities on the Internet, whether due to the way it recruited new fighters, propagated propaganda, or used encrypted applications for communication. However, it is not likely to pose a current threat as regards cyberterrorism. The 2016 National Security Audit defined cyberterrorism as a cyber attack that "threatens the functioning of the state, its constitutional system or defence capability, inter alia by targeting critical information infrastructure and major information systems". Such an attack would require advanced cyber capabilities that terrorist groups are unlikely to have at the moment, and the corresponding investments of both human and financial resources. Conventional attacks are increasingly effective for terrorist groups, while also bringing more attention at less effort and cost.

Hacktivists:

These are political activists who undermine the availability, credibility or integrity of information with a view to political, ideological or social change. These are often DDoS attacks, defacement, hacking into accounts on social networks or publishing personal data. In the **Czech Republic**, hacktivist attacks are in decline. One of the most recent activities was the Czech Blockade by a branch of Anonymous which took place in 2016. It was launched against Czech politicians and government institutions in response to the approval of the Gambling Act. In this case, the National Central for Organised Crime carried out a successful operation, accusing 6 people of criminal activities.

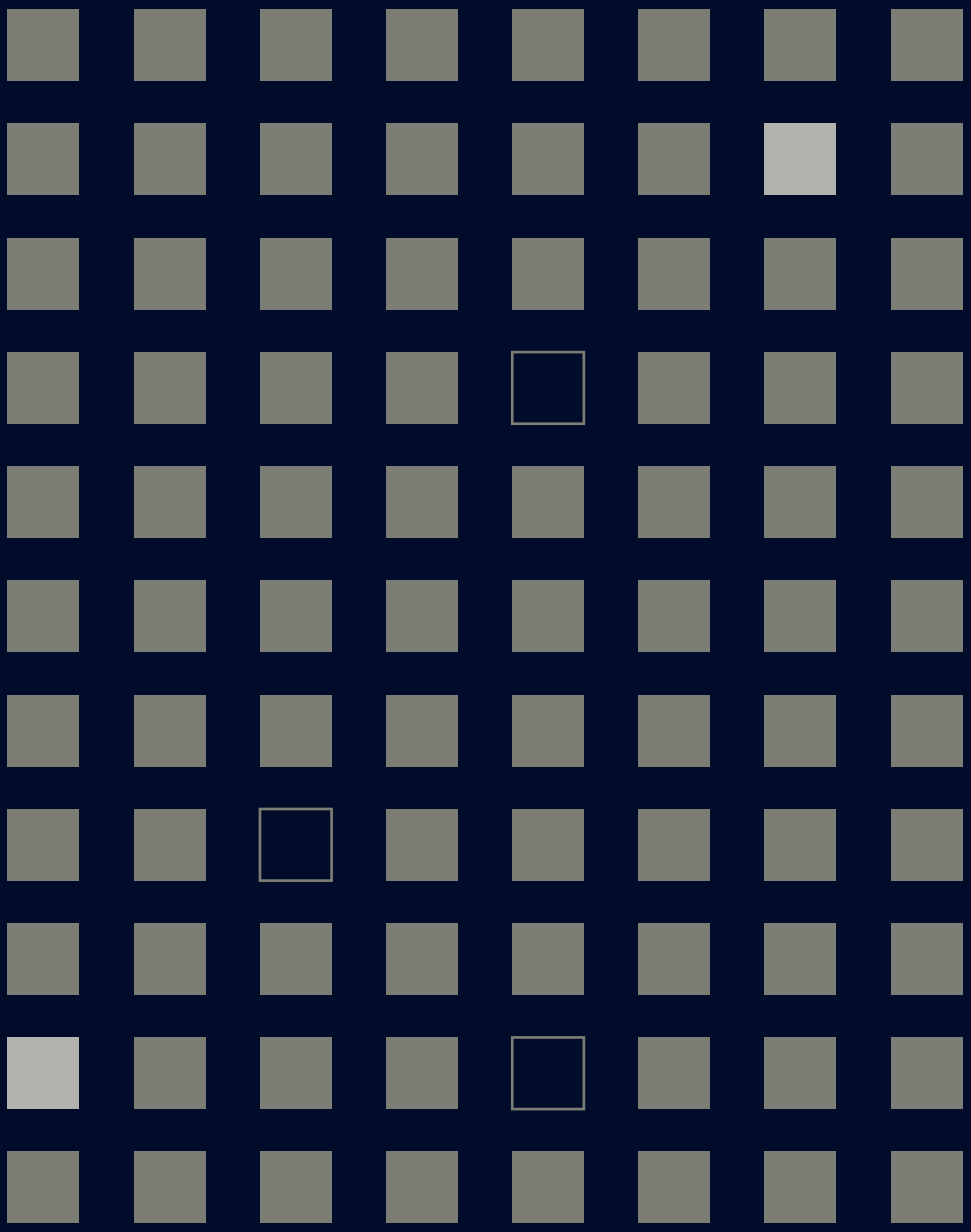
Black hats:

Black Hats are also active actors in the **Czech Republic** and abroad. These are hackers who do not work for any interest group, but tend to pursue their own interests through attacks, such as gaining recognition in the hacking community or financial gain.

Script kiddies:

Another group in the Czech Republic and abroad is script kiddies, a slang term for amateurs who use tools developed by other attackers to carry out their own attacks.

Cyber threats



Cyber espionage: state actors in Czech networks

Impacts	loss of data, compromise of sensitive and classified information, loss of trade secrets leading to loss of competitiveness
Attacker	state actors, state-sponsored groups
Methods	zero-day vulnerabilities, advanced spear-phishing campaigns, watering-hole attacks[2] and others

Cyber espionage means the whole range of malicious activities in cyberspace that aim to access sensitive or classified information and then use that information for the benefit of the attacker. The most common actors in cyber espionage are Advanced Persistent Threat (APT) groups.

For cyber espionage, social engineering methods are the most frequent attack vector leading to the initial penetration of the system, most commonly spear-phishing (for more information on spear-phishing see page 24).

Successful cyber espionage is a serious security incident that can have significant consequences:

Leaks of sensitive information:

Such information may include strategically important information for the state, the credentials of employees of organizations, and patents and know-how of research and private companies;

Preparations for more serious attacks and operations:

Information stolen through cyber espionage can be abused for further attacks. If an attacker is tied to a state actor, it is possible they will use the data to prepare further intelligence operations, both at the level of targeted cyber attacks such

APT groups

The advanced nature of APT groups does not lie primarily in their attack methods, but in the ability to remain unnoticed in the victim's system for months or years.

Most often they are state actors seeking to obtain classified information or trade secrets from other states, but there are also known cases of APT groups without state links that can act in the interests of specific private companies, or steal technology to sell to anyone who pays the most. Such cases more resemble industrial espionage that is closer to cybercrime than the common understanding of classical espionage.

[2] In a watering-hole attack, an attacker identifies a web site that his victim often visits and, if there is a vulnerability, infects it. Then, when the victim visits the infected site, malware is installed on their computer.

as spear-phishing and at the level of intelligence operations using human resources (HUMINT);

Distribution of infected content to other institutions:

If an attacker manages to access a victim's mailbox as part of their cyber espionage activities, they can use it to attack partner institutions, whether at home or abroad, through spear-phishing. The attacker can then benefit from using a legitimate e-mail address that inspires trust in the recipient. When an e-mail comes from a trusted organization's address, the chances that the recipient opens the malicious content and admits the attacker to their systems are also increased;

Access to other organization systems:

Stolen credentials can enable an attacker to access other institution systems, government systems, or systems of international organizations;

Basis for disinformation campaigns:

Obtaining often informal personal e-mail communications from top, politically active representatives of state can be an effective tool for discrediting them.

These consequences are illustrated by the successful breach of the COREU system (the communication network used by the EU Council, the European External Action Service, the Ministries of Foreign Affairs of the Member States and the Permanent Representatives to the EU and the European Commission) that occurred in 2018. Attackers managed to steal thousands of documents during the three years they had undetected access to COREU. According to the media, the case began in Cyprus. Through a phishing attack on an employee, the attackers accessed a Cypriot government system from they obtained credentials for the entire COREU system, and from there stole documents relevant to all 28 EU Member States.[iii]

The Czech Republic is not immune to cyber espionage.

In 2018 the NÚKIB continued its investigation into a large-scale attack on a strategically important Czech government institution. The investigation included an analysis of available technical data and other relevant information (character of the victim, duration of the attack, nature of stolen information, disposal of stolen information, etc.), concluding that the attack originator was almost certainly (90-100%) a state actor or a group associated with one. According to the information available to the NÚKIB, it is likely (55-70%) that the attack was conducted by a Chinese actor.

Data leaks: Countless possibilities for further abuse

Impacts	theft of personal data, its possible abuse for subsequent spear-phishing attacks, identity theft or credential stuffing (see below)
Attacker	state actors, state-sponsored groups, cybercriminals, script kiddies, terrorists
Methods	brute force attacks, SQL injection , and others

2018 was characterized by frequent leaks of personal data all over the world. Throughout the year there were reports of new leaks and the numbers of people affected (whose personal information was stolen) climbed to tens or hundreds of millions.

Data leaks are dangerous due to the possibility of further abuse. They may be abused for:

- A subsequent spear-phishing campaign that may increase the likelihood the victim will click on the link or download the infected attachment;
- Victim identity theft;
- Credential stuffing, when attackers try to use leaked user passwords to access their other accounts. If users use a single password for multiple services, this makes it easier for attackers;[4]
- Building a special region-specific password database that attackers can use for dictionary attacks
- Compiling kill lists through which terrorist groups call for the killing of people on such lists;
- Compiling blacklists on which extremists publish their enemies;
- Stealing funds from electronic wallets. Attackers search victims' e-mails for information about their electronic wallets, from which they subsequently transfer money to their own accounts; [vi]
- Distribution of spam and unsolicited advertising;

[3] SQL injection is a technique commonly used to attack databases. If an attacker puts their own command into a database query, they can do almost anything with the database – copy, modify, or delete it completely.

[4] As security expert Troy Hunt found, some credential stuffing lists contain over 100 million e-mail addresses.

A Czech example of the abuse of leaked data: Combining leaked passwords with spear-phishing

In the autumn of 2018, blackmail e-mails were spread through the **Czech Republic**, with attackers trying to convince users they had been filmed while watching pornography. They threatened that the recordings would be published if the users did not pay the set amount in bitcoins.

To increase the likelihood that people would pay, they employed data that had already been leaked. They targeted specific users through e-mails and added their stolen personal information and passwords to the text, trying to convince their victims that their computers had indeed been compromised, imparting in them a sense of urgency to pay the amount.

According to publicly available information about the wallets, the attackers netted almost USD 6,000 in this way, equivalent to CZK 130,000.

Attacks through supply chain weak points: Detours to the real target

Impacts	data loss, compromise of strategic information, threats to competitiveness, sabotage
Attacker	state actors, state-sponsored groups
Methods	phishing and spear-phishing targeted towards employees of suppliers

Attacks through supply chain weak points have been on the rise in recent years, and it has been shown that attackers are able to do considerable damage with their help.

A supply chain can be abused by attackers to gain access to state institutions and also to industrial or other entities. The reasons can vary – attempts to obtain data or system access with the intention of sabotage (causing material damage).

A supply chain is vulnerable at both software and hardware levels. At the software level, cyber attacks target a weak link in the chain to gain privileged access and use it to compromise the system at the end of the supply chain.

A widely discussed topic in 2018 was attacks on managed service providers, such as managed service providers (MSPs), which include cloud computing service providers. Attacks through MSPs are difficult to detect for a target organization that uses these services because the attacker is abusing a vendor's privileged access.

Supply chain security and the use of managed service providers (MSP) is also a relevant issue in the **Czech Republic**. Examples are state and private institutions governed by the Cyber Security Act [Act No 181/2014, on Cyber Security and on Amendments to Related Acts (Cyber Security Act), as amended (hereinafter the "CSA")] and that use or are planning to use MSPs. The solution is not to completely exclude service providers, but rather entities governed by the CSA are obliged to take into account, in their risk management, that the protection of their systems already starts at the level of security of their suppliers' systems. For this reason, the security of the service provider should be considered to the extent that it corresponds to the security of its own system, the supplier should be included in the risk analysis.

In the **Czech Republic**, the potential supply chain risk factor is the current method of application of the Public Procurement Act [Act No 134/2016, on Public Procurement, as amended (hereinafter the "PPA")], when procurement procedures with price as the main or sole criterion prevail. According to the questionnaires sent, the contacted organizations perceive this practice as reducing cyber security in their organizations. Under the CSA, lowest price offers mean that potentially hazardous components may enter the systems of obligated entities. However, the PPA in its current form allows for criteria other than price to be considered, but the application of these criteria requires, in many cases, greater capacity on the part of the contracting authority, and increases the risk of possible reviews, which may unduly prolong award procedures.

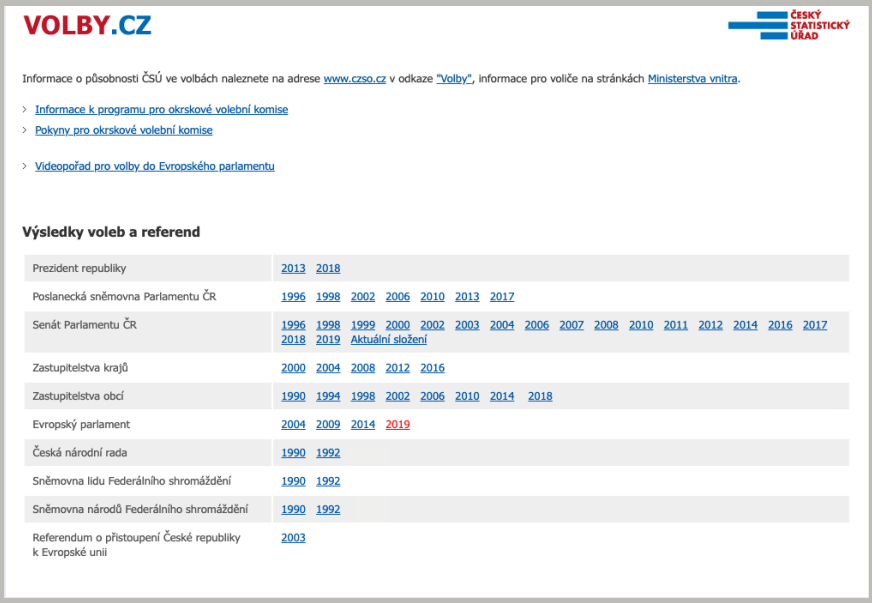
[5] *One example is the NotPetya malware that was spread through an update to accounting SW.*

Cyber attacks on the electoral process: Attacks on the basic pillar of democracy

Impacts	limiting the availability of election results, stealing politically sensitive materials to discredit candidates, disseminating misinformation, distrust of elected representatives, disrupting the processing of election results, reducing confidence in the democratic process
Attacker	state actors, state-sponsored groups, hacktivists, script kiddies
Methods	phishing, spear-phishing, DoS/DDoS

The events of the last three years have changed the view of many Western countries on the security of the electoral process. The cyber attacks on the US Democratic Party in 2016 and French President Macron's electoral staff a year later were watersheds in this regard. Politically sensitive documents from both electoral staffs were stolen and subsequently published, while some were falsified in the case of President Macron. The aims of the attackers in both cases was highly likely to discredit the presidential candidates.

The Czech Republic also has experience with cyber attacks on elections. During the parliamentary elections in autumn 2017 and the municipal elections a year later, there were DDoS attacks on public addresses of the Czech Statistical Office (CSO), which processes and provides information about the results of the elections. In 2017 a DDoS attack put the electoral websites volby.cz and volbyhned.cz out of action for several tens of minutes. The police leading the investigation were forced to set it aside due to lack of source data. [vii] A year later a DDoS attack on the official CSO website was carried out by an unknown perpetrator during



Website volby.cz on which DDoS attack was performed in October 2017 Source: volby.cz

municipal elections. Thanks to DDoS protection, the website remained available. Neither of the attacks affected the transfer of election results from the collection points to the headquarters, and therefore the independent data processing was not affected. However, their timing indicates the attacker's intention was to disrupt the result publication process.

Cyber attacks on elections are attacks on a fundamental pillar of democracy and can have far-reaching consequences. They can undermine the election results processing process, undermine the legitimacy of elected representatives and, in extreme cases, create voter mistrust in the democratic system.

The Czech Republic is aware of the threat posed by cyber attacks on elections and is taking measures to increase the security of the Czech electoral process. Further information on the measures is available on page 49.

DDoS: Exponential increase in attack strength

Impacts	disruption of service availability, financial losses, distraction from other attacks, damage to competitors
Attacker	cybercriminals, state actors, state-sponsored groups, hacktivists, script kiddies, terrorists
Methods	botnets, DNS amplification, SYNFlood[7]

The foundation of cyber security is to ensure the availability, integrity and trustworthiness of information. DoS (denial of service) and DDoS (distributed denial of service) attacks impact the first principle of cyber security – the availability of services and related information.

(D)DoS attacks are quite common. They accompany other cyber attacks, distract attention from other attacks, are used by hacktivists as a virtual blockade and protest, by private companies to weaken their competitors, or as a political tool to show disagreement. Moreover, the execution of DoS and DDoS attacks is relatively simple. If attackers do not have the ability to prepare such an attack themselves, they can now lease a botnet[7] as a service.

DDoS in 2018

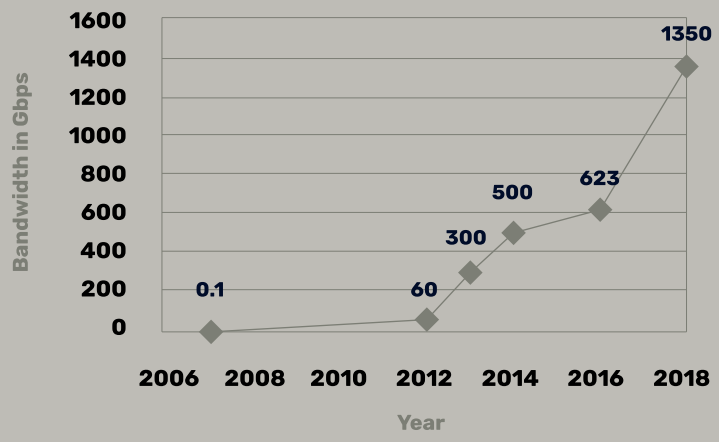
2018 became a watershed in DDoS attacks and their strength. At the end of February, there was a 10-minute failure of the Github platform when it was hit by a DDoS attack of up to 1.35 Tb/s. It was the strongest DDoS in history and the attack used a new method that takes advantage of incorrect settings of the **Memcached** server protocol.

As the strength of DDoS attacks increases (see the graph below), demands for protection against them also increase. **A DDoS attack that exceeds 1 TB/s would probably not only disturb the availability of compromised websites in the Czech Republic but would also affect the backbone line and related infrastructure.**

What is the difference between DoS and DDoS attack?

DoS (denial of service) and DDoS (distributed denial of service) attacks vary in the number of resources that generate them. In a DoS attack, usually one computer and one connection are used to overwhelm the victim's system by requests. DDoS uses more computers connected to the so-called botnet to overwhelm.

Development of DDoS attack strength



[6] *SYNFlood is a form of DoS attack in which an attacker sends a wave of SYN packets, which are used to establish communication between two systems, thus overwhelming the victim's system*

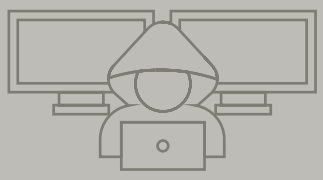
[7] *A network of infected computers controlled by a single hacker who thus has access to the computing power of many thousands of machines simultaneously*

How do Memcached DDoS attacks work?

Memcached is a publicly available tool used to improve the efficiency of communication between servers within an organization. Yet if administrators ignore the correct settings, run the service on the UDP protocol and leave its port open to the Internet, attackers can exploit it for powerful DDoS attacks. They scan the Internet, find unsecured Memcached servers, and send a request with a fake IP address to the victim. The Memcached system can multiply the size of this request by up to 51,000 times and thus the response the victim sends is many times larger than the request itself. It is relatively easy to overwhelm a victim's server in this way, especially when thousands of insecure Memcached servers are being exploited.

1

Attacker



Servers with unsecured Memcached ports

Destination port: UDP 11211
Size: X bytes
Request source: fake IP address of the victim
Request target: servers with unsecured Memcached ports

2

Servers with unsecured Memcached ports

The Memcached system responds to the request

Source of response: servers with Memcached ports
Request target: IP address of the victim
Size: n x X bytes (n = size multiplier)

3

Victim

DDoS in the Czech Republic

The attacks that hit Czech infrastructure in 2018 did not reach such strengths as abroad. These were mostly minor attacks of tens of Gbps, which either attacked an infected website for a few minutes or were completely halted by DDoS attack protection. Yet DDoS remains a frequent type of attack. Exactly half the respondents to the questionnaires in this report replied that they had detected DDoS attacks on their networks in 2018.

Several cases required attention in 2018:

A

A DDoS attack on the Czech Statistical Office website, described on page 16;

B

A DDoS attack on the website of a Czech consulate. The outage lasted several tens of minutes;

C

A series of DDoS attacks on Czech Internet providers, including the largest mobile operators. At the turn of 2018 and 2019, these were exposed to a wave of attacks targeting both their customers and them. The attacks were different from usual ones in that they did not target a specific service but rather different addresses and entities. They could therefore have only been to test the protection capacities in the **Czech Republic**. [viii]

Malware for illegal cryptocurrency mining: Growth at the expense of ransomware

Impacts	unlawful exploitation of victims' computing power with no clear impact on confidentiality and integrity, hypothetical limitations on the availability of information systems
Attacker	cybercriminals
Methods	attacks on the computational power of infected devices or attacks on websites using a visitor's computer

Cryptocurrency mining malware (also called crypto mining) is an emerging threat attacking computers, mobile devices and network servers, using the power of these devices to extract cryptocurrencies. The main motive of the malware is profit, but a significant difference from similarly motivated attacks is that it is designed to remain completely hidden from the user.

CoinMiner in the Czech Republic

The malicious CoinMiner application was a very common Internet threat in 2018. According to statements by some antivirus companies, CoinMiner was one of the most common Internet threats in the Czech Republic at the beginning of the year. CoinMiner exists in two versions. The first version runs on a website and uses a visitor's computer to extract cryptocurrencies, but the second version is more interesting because it uses the EternalBlue exploit to infect vulnerable computers. After a computer is successfully infected, WMI scripts are run. WMI scripts run only in the infected computer's memory and are therefore more difficult to detect. Using these scripts, additional malicious code is downloaded to the victim. There is already a patch available for EternalBlue, but given the impact of CoinMiner it is clear that there are still computers that have not been updated.

In crypto mining, there are three main ways of infection:

1

A website is infected and cryptocurrency is mined by victims through their browser while visiting an infected page. In some cases, the victim's equipment temporarily continues to mine even after leaving the infected site;

2

An attacker uses an existing botnet to install a crypto mining module on previously infected computers;

3

Malware exploiting vulnerabilities, etc. to spread over a network.

Crypto mining vs. ransomware

Unlike ransomware attacks, cryptographic mining through malware does not require an attacker to communicate with the attacked entity (e.g. to provide their ability to decrypt the infected data), nor does it require any specific action on the part of the victim, or willingness to pay a ransom. Compared to ransomware attacks, attackers risk less from a criminal-law perspective, as blackmail is not part of the crypto miner's attacks and the likelihood of human lives being ultimately threatened is extremely low. The rising trend of crypto miners suggests that this could generally be a more efficient tool for generating financial gain, making it more attractive to attackers than ransomware. Despite the impact on the computational performance of the victim's infrastructure, these attacks are less serious from the ICT protection point of view. Unlike ransomware attacks, they are not destructive and do not compromise the availability of important data. It is in the attacker's interest to ensure the crypto miner takes so little power that the victim does not notice it at all.

Infection by crypto miners is a **growing trend noted across most sectors, including in the Czech Republic.**

Targets of cyber attacks

02

Users: Gateway to an organization's network

Impacts	providing attackers with access to an organization's network
Attacker	state actors, state-sponsored groups, cybercriminals
Methods	phishing, spear-phishing, watering hole

In the field of cyber security, it is the end users of information technology that are usually considered most vulnerable. Attackers are aware of this weakness and exploit users as gateways to the networks of organizations they want to compromise. Attacks against users mostly use social engineering, the technique of manipulating a person to behave in a way that is not in their interest. In the context of cyber security, this is usually an effort to obtain specific information (e.g. a password) from the target victim or to persuade a user to download attachments that include malware. Phishing and spear-phishing are the most widely used social engineering techniques in cyberspace.

Phishing:

This type of social engineering takes the form of an e-mail, SMS or social network message in which an attacker tries to persuade a victim to disclose sensitive information, open a link to a malicious page, or open an attached file containing malicious code. Unlike spear-phishing, it is not personalized and is usually sent to a large number of people at once.

Spear-phishing:

This is a personalized form of phishing that targets specific individuals. The attack requires more preparation, for example the attacker must identify a specific person in the organization to whom they send a phishing email. At the same time, the attacker must have sufficient knowledge to create an e-mail that will be credible and not seem suspicious to the victim. Spear-phishing is one of the primary techniques that APT groups use to gain access to a target network, whether for espionage or to cause damage.

A physical form of spear-phishing (the method also known as "Baiting") is the presence of a seemingly discarded USB drive near a target, such as in the employees' car park. The attacker relies on the curiosity of the employee who finds the drive, hoping they will connect it to a work computer connected to the target network. The drive may contain, for example, malicious code that allows the attacker to access the network.

The sophistication of targeted phishing attacks in the **Czech Republic** increased in 2018. While phishing is still most widespread through e-mails in broken Czech, the number of spear-phishing attacks is growing, and it is clear that the perpetrators have an excellent knowledge of the environment and have invested a lot of time in preparing such attacks (e.g. by creating fake websites identical to legitimate ones). Financial institutions and their clients are frequent targets of phishing attacks in the Czech Republic, but in recent years the proportion of attacks against Czech universities has increased (for details on phishing attacks on Czech universities, see page 38). The main motivation of the attackers is financial gain, but efforts to steal intellectual property are no exception.

An example of not very sophisticated phishing in 2018 was threatening e-mails in which the attackers told their victims they had obtained sensitive footage through a webcam and threatened to publish this footage. To prevent this, the victim should send them a certain amount in bitcoins. [ix]

However, this is not purely a problem of the users themselves. In a number of private companies, public institutions and non-profit organizations, cyber security is not given enough attention and employees lack the necessary training in digital hygiene principles that employers should provide.

Public sector: A slowly adapting environment

Impacts	loss of data, compromise of sensitive and classified information
Attacker	state actors, state-sponsored groups
Methods	phishing, spear-phishing, DDoS, and others

The public sector, especially state institutions which provide attackers with intelligence, military, and politically and economically important information is a frequent target of cyber attacks. Cyber spy operations seeking such information are of a long-term nature and require the attackers to have an advanced ability to avoid detection over the long term and acquire data from the infected system unnoticed. This level of know-how is mainly available to state actors or groups sponsored by them, which is unlikely to change in the future, nor is their increased interest in state institutions.

The Czech public sector has a number of specific influences that distinguish it from common private sector principles. These factors are reflected in the principles of the normal function of individual state institutions and directly or indirectly affect the level of cyber security in them. This means:

Uncertainty in the near future:

Changes arising from election results often mean stopping current activities and waiting for new leadership, procedures and approaches, including in ICT operations or cyber security;

Prioritizing short-term goals over long-term goals:

The main tendency is to implement what can be immediately seen. Strategic projects that will take effect over a long period (relative to the previous point) are more difficult to implement;

Table-based salaries and insufficient personal remuneration or rewards:

The salaries of public sector experts generally cannot compete with those in the private sector.

The most common vulnerabilities in the Czech public sector include:

A lack of cyber security experts, mainly due to the non-competitiveness of the public sector in offering financial remuneration and employee benefits.

- **Example:** Cyber security salaries in the private sector are generally higher.
- **Risk:** Overworked individuals on which the institution's cyber security is built.

Insufficient deepening of the knowledge of staff responsible for the operation, management or security of ICT resources, due to the low training budget for these staff.

- **Example:** The assumption by top management that the cost of training for officials and ICT professionals is comparable. Common training for officials usually costs several thousand crowns, while training in ICT operations and security usually costs tens of thousands of crowns. Top management then does not permit such expensive training, or permits it only sporadically.
- **Risk:** ICT experts do not know the current trends in cyber security, which can make it easier for a potential attacker.

Organizational conflict of interest in responsibilities for ICT management and ICT security

- **Example:** The person administering a security measure also checks the security of such measure.
- **Risk:** A lack of adequate control as to whether a measure really serves its purpose and is sufficiently effective.

Time to promote and approve security plans

- **Example:** The approval of a new security policy/directive in many institutions takes a year or more.
- **Risk:** When such a policy/directive is not approved and effective, it is not enforceable and employees do not have to follow it.

Different rules for top management

- **Example:** Top management has administrator privileges and permissions to use ICT devices, such as the ability to install executables, for their convenience in some institutions.
- **Risk:** Top management does not check if the executable file they install contains malicious code. Installing such software may disrupt the operation of the institution's entire internal network.

Use of weak authentication (login) mechanisms

- **Example:** Logging users into information systems is performed only based on username and password, even in critical systems.
- **Risk:** Today this is an outdated authentication mechanism with many weaknesses, for example a user who writes a password on a piece of paper next to the monitor or chooses a weak password that can be quickly guessed by performing a dictionary attack or by transferring and storing the password itself.

Critical infrastructure: Attacks on the smooth functioning of the state

Impacts	violation of confidentiality, availability or integrity of information in networks important for the operation of the state
Attacker	state actors, state-sponsored groups
Methods	phishing, spear-phishing, watering hole, zero-day vulnerabilities

According to Section 2 of the CSA[x] critical information infrastructure (CII) means a critical infrastructure (CI) element or system in the field of communication and information systems in the area of cyber security. According to Section 2 of Act No 240/2000, on Crisis Management and on Amendments to Certain Acts (the Crisis Act)[xi] , critical infrastructure itself is defined as an element or system of elements whose disruption would have a serious impact on national security, the needs of the population, human health or the economy of the state.

Critical infrastructure information systems have long been a favourite target of cyberspace attackers. Attacks on such targets require a high degree of sophistication, time-consuming preparation and extensive resources, and therefore remain the domain of nation states or groups sponsored by them. CI is an inviting target for attackers. Paralysis of one or more elements can inflict serious damage on the target state and can be strategically beneficial to the attackers. Traditional CI elements include power plants, dams, airports and telecommunications networks. The elimination of any of these elements may paralyse a state's ability to provide services (electricity, heat, water) or defend itself against conventional attack.

According to information available to the NÚKIB, there has not been any sophisticated and focused cyber attack targeting CI in the **Czech Republic**, but the same cannot be said about other states. While there have been no serious attacks with dramatic impacts as in the past, cyber security institutions issued a series of warnings in the course of 2018 regarding ongoing attacks, such as:

- In April 2018, the US Department of Homeland Security, the FBI and the British National Cyber Security Centre issued a joint technical alert regarding attacks on their critical information infrastructure administrators and Internet service providers. In particular, network devices (routers) were the subject of the alert as they are ideal targets due to a combination of relatively weak protection and extensive network access. The alert stated that the attacks came from groups sponsored by the Russian Federation.[xii]

[8] Such as the December 2015 attack in Ukraine, when over two hundred thousand people were left without power as a result of a cyber attack.

- In December 2018 Australia, Japan, Canada, New Zealand and the United Kingdom issued alerts regarding ongoing cyber attacks on health, defence, energy and telecommunications entities. According to the alerts, the APT10 group with links to the PRC was behind the attacks.[xiii]

Given the importance of critical infrastructure and the existing interests of various actors, similar attacks cannot be excluded in the future.

Concentrated attacks on CI usually have several characteristics. Attackers most likely get access to victim systems through social engineering (phishing, spear-phishing, watering hole), they operate in the system for a long time in order to collect the necessary information, and their ultimate aim is to obtain sensitive data or take control of the industrial control systems in individual CI components.

It is precisely through infecting control systems with malicious code that attackers can control the attacked CI element, disable it, or, in extreme cases, cause material damage and loss of life. Industrial security systems can also be targets of CI attacks. These are targeted, for example, by the Triton malware (also Trisis, Hatman) that was found in a petrochemical facility in Saudi Arabia in 2017. In 2018 the FireEye cyber security company traced its origin to the Russian Federation.

Triton/Trisis malware targeting industrial security systems

Triton was first discovered at the end of 2017 in Schneider Electric's Triconex safety instrumentation system[9] in a petrochemical facility in Saudi Arabia. It is the first malware of its kind that does not target programmable logic controllers[10] ,but attacks safety systems. Safety systems are designed to detect an imminent threat of an accident and, by means of appropriate countermeasures, take the necessary measures to return the process to a safe state. A safety system infected with malware may not assess a crisis situation (overpressure, overheating) as a danger and this could result in an accident and consequently material damage or loss of life. In the case of the attack on the petrochemical facility in Saudi Arabia, the malware was detected thanks to a coding error and failed to do any damage.

The origin of the malware was traced by FireEye experts in 2018 to a Russian scientific institution with links to the Ministry of Defence, the Central Institute of Science and Research of Chemistry and Mechanics. [xiv]

Triconex device by Schneider Electric

[9] Also, Safety Instrumented System (SIS)
[10] Also, Programmable Logic Controller (PLC)

Energy sector: The field of attack expands[11]

Impacts	electricity gas outages, information leaks
Attacker	state actors, state-sponsored groups
Methods	phishing, spear-phishing, watering hole, zero-day vulnerabilities

The energy sector is a difficult but attractive goal for attackers. If network operators in the energy sector adhere to cyber security principles and separate industrial control systems from corporate networks (non-manufacturing and non-production networks, including the Internet), cyber attack is very difficult. On the attacker's side, it requires both sophisticated cyber capabilities and significant time and financial resources. Nevertheless, the number and sophistication of attacks on the energy sector is increasing (see the timeline below). The chance to control the supply of electricity in an enemy's grid is especially attractive for state actors.

The power industry environment is so specific that there may be combinations of vulnerabilities that an attacker can exploit.

Obsolete components:

The first is associated with the industrial control technologies themselves. These are special electrical devices whose life cycle can be planned for many (often over ten) years ahead. Thus the system may contain obsolete components from a cyber security perspective;

Updates:

Outdated control devices are associated with the issue of firmware updates. Updates are not often released by device manufacturers as frequently as in IT, and when they are released there may be a problem with their installation because, as in IT, the update should initially be tested in a non-production environment. To prevent power outages, power plant systems are not shut down outside planned shutdowns, so updates may be delayed;

Supply chain attacks:

The supply chain may also pose vulnerabilities in the energy sector. In some cases, industrial control systems remain connected to supplier networks, enabling suppliers to obtain data from real-world installed equipment, e.g. for diagnosis (ascertaining the condition of the equipment, its utilization, wear, etc.). Yet these inputs create an opportunity for attackers to gain access to utility networks through supplier networks.[xv]

[11] Every year the report on cyber security focuses on those sectors of critical information infrastructure about which new knowledge will emerge.

China's cyber espionage suppliers to the power industry

Industrial control equipment manufacturers are also an attractive target for cyber espionage. In 2017, the US Department of Justice accused three citizens of the People's Republic of China of cyber spying against Siemens which supplies industrial control equipment to the energy sector. The legal action specifically stated that the company's energy division was one of the targets of the attackers. This was probably cyber espionage, but it cannot be ruled out that the attackers were collecting information to prepare attacks of a destructive nature.

In the Czech energy sector there is a new SMART technologies trend that distribution companies are starting to deploy across the country. Smart electricity meters (SMART meters) can record energy (or water and gas) consumption and automatically send their data to a central office for processing. For the distributor this means an opportunity to optimize energy flows, for the hacker the possibility to expand the field of attack with new targets. If SMART meters have the functionality to remotely disconnect non-payers, it will be possible to exploit any insufficient security to inflict general electricity or gas outages. SMART meter manufacturers should therefore ensure their devices are adequately secured to minimize the risk of cyber attack.

Malware targeting industrial control systems in the energy sector

2014

Havex (Europe and the USA)

Havex (Europe and the USA): The companies attacked by Havex were engaged in remote management systems for ICS systems, indicating that the attackers were looking in their networks for information they could use to further attack the energy sector. There are no reports that the malware caused physical damage.[xvi]

2015

BlackEnergy (Ukraine)

The attack the day before Christmas is considered to be the first cyber attack to successfully cause a power outage. The attackers managed to compromise the networks of three Ukrainian distribution companies, causing a temporary power outage affecting more than 200,000 people.[xvii]

GreyEnergy (Poland)

ESET detected GreyEnergy, BlackEnergy's successor. Its first target was an unspecified energy company in Poland.[xviii]

2016

Industroyer (Ukraine)

Ukraine was also the victim of the Industroyer malware (also known as Crashoverride), leaving a fifth of Kiev without electricity. It was sophisticated malware that enabled attackers to control electricity distribution through industrial communication protocols. According to experts it was a test in which the attackers tested their capacities.[xix]

2017

Cyber attacks on US and German energy companies (USA and Germany)

In 2017, US and German energy companies faced constant attempts to compromise their networks. The initial victims were suppliers exposed to a wave of spear phishing and watering-hole attacks. Through them, hackers attacked their primary goals – energy distribution companies and other critical infrastructure entities. Their goal was not only to collect information but also disrupt industrial management processes.[xx]

TRITON (Saudie Arabia)

More about the TRITON malware on page 29.

2018

GreyEnergy (Poland and Ukraine)

GreyEnergy's attacks returned and energy and transport companies in Ukraine and Poland were targeted.

Banking sector: A secure yet very tempting target

Impacts	financial loss, loss of bank reputation, disruption of business continuity, loss or unauthorized change of data
Attacker	cybercriminals
Methods	phishing, spear-phishing, insertion of Trojan malware into legitimate mobile applications

The Czech National Bank conducts regular cyber security checks in the banking sector. The absence of more serious incidents means we can conclude that the **Czech banking sector** is relatively well secured. However, there are still differences in the maturity of individual financial institutions, in particular in terms of protection against advanced cyber threats and internal intruders (e.g. in security monitoring and penetration testing). In general, however, banks try not to underestimate cyber security, as the compromise of their information systems could have far-reaching financial and reputational consequences.

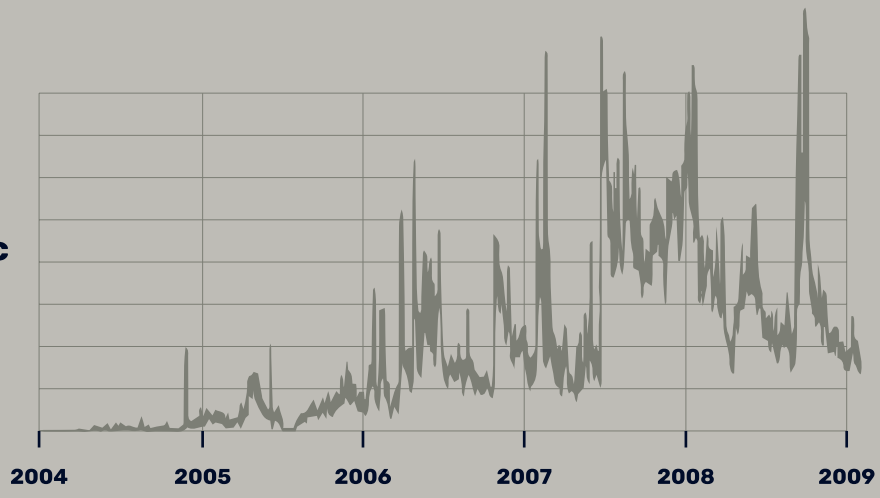
Clients themselves were the greatest vulnerability in the banking sector in 2018. Attackers often exploited this long-term weak link and, in 2018, banks saw an increase in the number and sophistication of phishing and spear-phishing attacks on their clients.

Another weak point is, in some cases, deficiencies in the effectiveness and speed of response to cyber incidents (attacks) in terms of the coordination and capacities of bank CERT teams and the preparation of well-tested incident management plans.

Attacks on mobile internet banking are becoming a new trend. More and more people use mobile applications to manage their finances, and hackers have quickly adapted to this. ESET's telemetry data clearly shows that malware targeting Android banking applications is increasing.

Graph 3:

Increase in banking application malware on Android OS in the Czech Republic and abroad [xxi]



Source: https://www.welivesecurity.com/wp-content/uploads/2019/02/ESET_Android_Banking_Malware.pdf

In 2018 one example of this trend was the QRecorder application, which damaged Czech bank clients. This application, available in the official Google Play store, was used to record calls. After an update, QRecorder was modified to behave like a Trojan application.

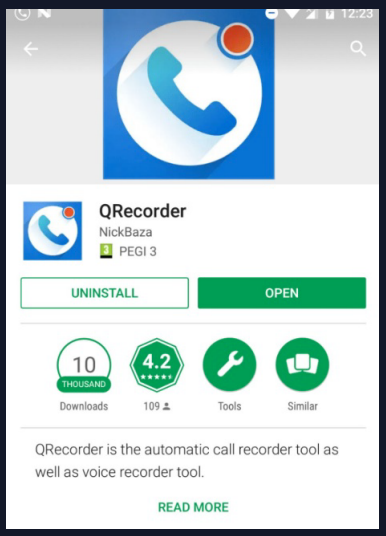
The modification of legitimate applications to become trojans is potentially a very serious problem. A large number of independent developers place applications on the Google Play store and sell the rights to the applications. In the case of the QRecorder application, the attackers paid USD 29 (about CZK 650) for the application source code. This is a relatively low cost that allows cybercriminals to exploit legitimate malware applications.

QRecorder under scrutiny

Security analysts have found that after an update QRecorder was redesigned to behave like a Trojan application. With this modification, attackers could remotely access a smartphone on which the application was installed. In addition, they had the ability to scan entered credentials and read SMSs to obtain both the necessary factors for authentication to various services, such as mobile banking.

The malware initially detected whether there were applications on the phone that could be monetizable for attackers, such as banking applications. Subsequently, a module was downloaded to the phone that created an invisible layer above the target application (e.g. internet banking) and captured the user's credentials.

The way in which the legitimate QRecorder application was turned into a security risk is extremely insidious. The attackers legally purchased the source code from the developer of the original application on the Google Play store and replaced it with an almost identical application with the same name. When the attackers injected malicious code into the application, they raised no suspicions.



eHealth: Attacks on the most sensitive personal data with life-threatening potential

Impacts	unavailability of critical data with possible impacts on the efficacy of healthcare facilities and on patient health; in the case of attacks on data confidentiality, the possibility of extortion and, in the case of publication of the data, interference in patients' personal lives
Attacker	cybercriminals, probably state actors
Methods	phishing, spear-phishing, unauthorized use of access data, ransomware

Due to the sensitivity of the data and the possible impact of eHealth attacks on patients' health and personal lives, the risks from threats to information systems used in healthcare are relatively higher than other systems processing personal data. The greatest threats include altering, stealing or losing sensitive patient personal data, along with the increased incidence of ransomware causing unavailability of important information. The security of medical IoT devices and the possibility of their abuse is also becoming a challenge.

Altering or preventing access to the increasing amount of digitized medical information can directly endanger patients' lives. Leaks and abuse or, in extreme cases, the disclosure of health information about a patient, is considered to be a serious attack on their personal life, which may harm an individual in their personal and public life. Many entities managing health information systems, especially health service providers, often lack the financial and staffing capacity to adequately secure the data they manage. This combination of facts means that **cyber attacks against health systems can provide relatively high profits at relatively low cost and effort.**

There are several risks in **Czech healthcare:**

A lack of cyber security standards

The problem of cyber security standards for individual health service providers has not yet been sufficiently addressed in the Czech Republic. In September 2017 the Ministry of Health issued methodological material on cyber security in healthcare in an effort to overcome this gap. As it was not binding, only a limited impact can be expected. From 1 August 2017 an amendment to the CSA came into effect, to include hospitals with a capacity of more than 800 acute beds or the status of a centre of highly specialized traumatological care whose information systems also meet predetermined requirements; the rest, however, remain unregulated.

Outdate software

One common feature of a considerable number of information systems used in hospitals is outdated software.

Risk of data theft

As part of the healthcare process, a large number of people from both employees and suppliers access sensitive patient data. Health service providers where proper management and control of information access is not established increase the risk of potential data theft and further monetization on the black market.

The most common types of attacks in **the Czech healthcare sector** include phishing and spear-phishing attacks which, according to the entities contacted, represent up to 90% of recorded attacks. The adopted technical measures are reducing the number of phishing attacks, yet the sophistication of spear-phishing attacks is increasing, while frequent targets are economic departments in healthcare facilities responsible for the finances of the organizations.

The Czech healthcare system also recorded a ransomware attack when the Tuberculosis and Respiratory Diseases Therapeutic Institution in Janov, Rokycany, was hit with a blackmail attack at the end of June 2018. Staff lost access to the institution's information systems. A payment in cryptocurrency was required to decrypt the files.

Academic world: Cyber attacks on the rise

Impacts	intellectual property leaks, economic loss, or unavailability of scientific equipment due to server outages
Attacker	cyber criminals, state-sponsored groups
Methods	phishing, spear-phishing, fraudulent e-mails, DDoS

The Czech academic world is an attractive target for cyber actors interested in intellectual property for several reasons:

- Universities often do cutting-edge research, accumulate know-how, and gather leading scientists in their fields;
- The security of Czech universities varies. There are no uniform security rules in the Czech Republic that all universities adhere to. CESNET provides advice and best practices, but implementation depends on the foresight and financial situation of the institution, and also on the willingness of the employees concerned;
- Due to the high number of users, university networks pose a particular challenge for security teams. There are thousands of students at Czech universities and most lack an awareness of cyber threats and how to prevent them. Their accounts can be abused just like university staff accounts, and hackers have lots of opportunities for compromise attempts.

cesnet

An association of universities and the Academy of Sciences of the Czech Republic that operates and develops a national digital infrastructure for science, research and education, comprising a computer network, computing grids, data storage and collaborative environments offering a wide range of services.

2018 clearly showed that hackers are interested in the **Czech academic world**. Ten Czech universities reported being exposed to a wave of phishing and spear-phishing attacks.

The phishing attacks of 2018 showed an increase in sophistication, with the attackers demonstrating detailed knowledge of the environment of Czech universities instead of a generic e-mail written in bad Czech. The attackers acted as real university employees, and the fraudulent sites to which the phishing and spear-phishing e-mails linked precisely copied the visual style of each workplace.

There is a lot of sensitive information in the **Czech education system** that can leak even without the involvement of an attacker. In 2018 inadequate personal data management resulted in the confidential information of up to 140,000 secondary school pupils being accessible through the Czech School Inspectorate InspIS application. Information that can be retrieved from the Czech School Inspectorate database includes name, surname, class and information on medical issues (without data on specific problems). The data leak was probably due to a technical error in the InspIS application. According to media reports, the fact that the application authors had not updated it for a year also contributed to the leak.

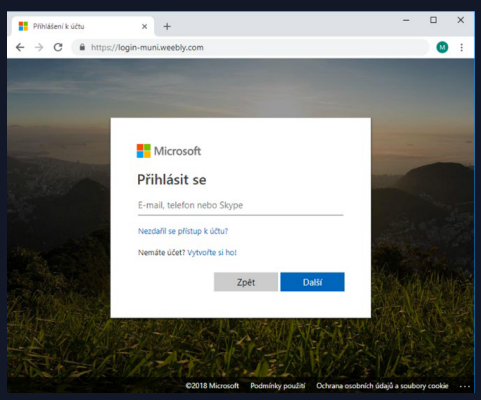
Cyber attacks on educational and research institutions must not be underestimated. If university networks are compromised, intellectual property and research results not yet published may be leaked. If attackers were to remain undetected for a longer period of time in the networks of **Czech universities**,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

Phishing at Czech universities

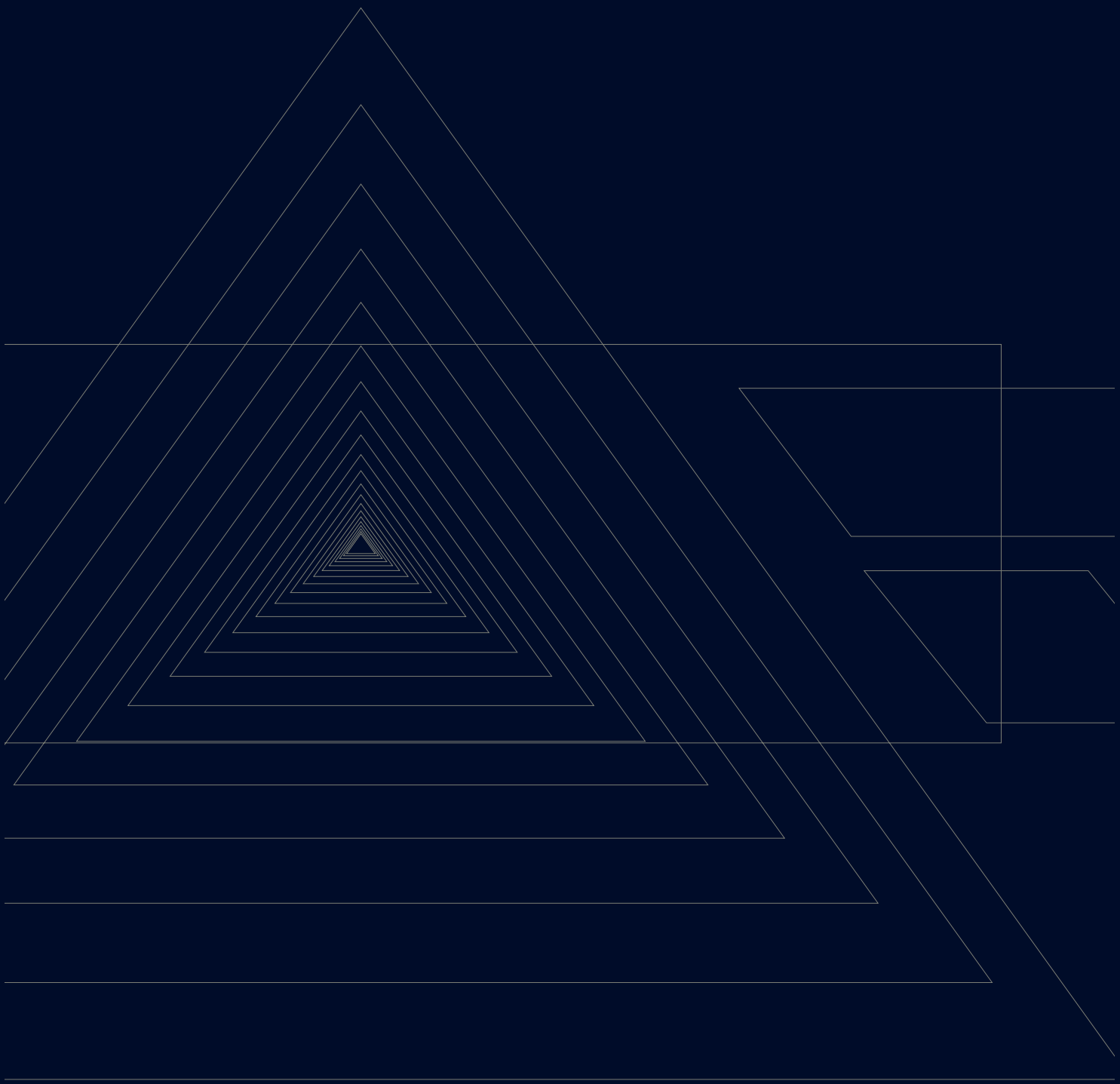
In September 2018, the Masaryk University Security Team (CSIRT MU) warned about a phishing campaign involving several Czech universities aimed at stealing research data, unpublished results and research group know-how. The target was data from a variety of disciplines such as medicine, engineering, and the humanities.

These were well-prepared attacks in which the attackers showed their knowledge of the environment of Czech universities. While the phishing e-mail text was not written in good Czech and contained a large number of errors, it appeared to be from the real university IT department and used the name of the real administrator, including his photograph, creating an impression of credibility.

The attackers asked their victims to activate their Office 365 accounts, which had allegedly been temporarily closed due to ongoing phishing attacks. They should use the link in the e-mail to activate them. However, it was in fact a link to a fake site that looked like a real Office 365 login page. If the victim entered their credentials on the spurious site, the attackers would also be able to gain access to the university's networks. According to the available information, no compromise occurred.



Source: https://csirt.muni.cz/about-us/news/phish_sci



03 Measures

Cyber and information security legislation: Setting basic rules for important entities

The protection of cyberspace is largely dependent on the legislation the relevant entities are obliged to comply with. In terms of the Cyber Security Act, these are entities whose information systems are important for the functioning of the state. These entities fall into the following four categories:

A	B	C	D
Critical information infrastructure	**Basic service**	**Important information system**	**Digital service provider**

Each of these four categories is discussed in Annex 3.

Legislation relating to the following entities:

- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 con cerning measures for a high common level of security of network and information systems across the Union (NIS Directive)
- Act No 181/2014 Coll, on Cyber Security and on Amendments to Related Acts (Cyber Security Act)
- Decree No 82/2018 Coll, on Security Measures, Cyber Security Incidents, Reactive Measures, Filing Requirements in the Area of Cyber Security and Data Destruction (Cyber Security Decree)
- Decree No 317/2014 Coll, on Important Information Systems and their Determining Criteria
- Decree No 437/2017 Coll, on Criteria for Determining the Basic Service Operator
- Commission Implementing Regulation (EU) 2018/151 of 30 January 2018

The identification of information systems falling within the competence of the CSA is still ongoing, and the number of obliged entities is increasing. At the end of 2018 the figures were as follows:

Number of designated entities at the end of 2018:

Critical information infrastructure entities:

45

entities

Critical information infrastructure elements:

114

information systems

important information systems:

178

information systems

Basic service operators:

30

entities

Basic service information systems:

30

information systems

NÚKIB methodical support on the web

The NÚKIB regularly publishes on its website supporting materials or schematics concerning the interpretation of the Act on Cyber Security aimed at simplifying cyber security issues for the professional and general public.

NÚKIB warning: Measures against imminent threats

One of the NÚKIB's tasks is to issue warnings about cyber security threats. The NÚKIB issues such warnings when it learns, in particular through its own activities, on the initiative of the national CERT operator or from authorities operating in cyber security abroad, about a cyber threat to which it is necessary to respond immediately.

Such a warning was the one dated 17 December 2018 against the use of Huawei Technologies Co., Ltd. and ZTE Corporation technical and software resources. Its publication was the result of a combination of knowledge and findings, described in more detail on the NÚKIB website.

The NÚKIB issued supporting methodology for this warning, which specified the measures that could be taken by the administrators of information and communication systems under the CSA. One measure also concerned the Public Procurement Act (PPA), which organizations often apply with price as the main criterion. However, the PPA in its current form allows for criteria other than price to be considered, but the use of such criteria requires, in many cases, greater capacity by the contracting authority and increases the risk of possible review, which may unduly prolong the award procedure. In 2017 the NÚKIB published support material for ICT public procurement, in which some security measures within the framework of the PPA are precisely discussed.

The full text of the Warning and related methodological support is available here:

https://nukib.cz/cs/informacni-servis/aktuality/1303-software-i-hardware-spolecnosti-huawei-a-zte-je-bezpecnostni-hrozbou/

https://nukib.cz/cs/informacni-servis/aktuality/1320-metodika-k-varovani-ze-dne-17-prosince-2018/

In addition to the warning pursuant to the CSA, a warning against the use of technology from Huawei Technologies Co., Ltd. and ZTE Corporation, the Agency regularly informs the public on current cyber threats on its website.

Cyber security exercises: Preparing for crises

Whole-of-government approach

This indicates an approach where institutions across government work together to achieve a common goal and a unified solution to a specific issue.

Exercises play an irreplaceable role in ensuring the cyber security in the Czech Republic. They faithfully simulate different types of crisis for both technical staff and top-level decisionmakers.

Close cooperation with other partners within the framework of a whole-of-government approach is essential for their creation and implementation. The NÚKIB, as a national authority, is responsible for cyber security exercises but cooperates with a number of partners in their preparation. In addition to the educational element of the exercises, they help build trust, strengthen relationships and identify existing deficiencies in cyber security processes.

The main benefits of the exercises:

1

The exercises give the **NÚKIB** the opportunity to identify and highlight weaknesses or shortcomings in cyber security. The crisis scenario method makes it possible to better outline possible negative impacts;

2

Based on the identified shortcomings and weaknesses, they contribute to the design, implementation and back-testing of specific new or modified solutions. In other words, exercises are an **excellent tool for validating and revising policies and processes,** e.g. on institutional and legal frameworks, crisis management, media communication, etc.;

3

Regular exercises greatly assist the NÚKIB in **mapping out approaches** and understanding various issues raised by institutions as well as their level of ensuring cyber security in the Czech Republic;

4

Exercises are an invaluable **resource for exchanging new knowledge, experience and technical skills;**

5

The knowledge learned and know-how gained are shared with other relevant actors. Exercises help **identify, define and confirm specific trends in the field.** Sharing also further enhances mutual cooperation and trust;

6

The outputs of the exercises represent valuable knowledge that can then be used for the **preparation of further public awareness raising and educational activities;**

7

Thanks to the demand and responses from foreign partners such as the United States of America, South Korea and Taiwan, the exercises have become an **important product with potential for Czech foreign policy.**

Cyber security exercises in 2018

Number of exercises organized by the NÚKIB:	Number of international exercises in which the NÚKIB participated:	Number of participants in exercises carried out by the NÚKIB
11	**3**	**320 from 77 countries**

Findings from the exercises that took place in 2018:

1.

There is a need to systematically and regularly raise awareness of cyber security among national security staff, including middle and senior management. It should be noted here that the problem of low awareness regarding cyber security is faced by almost all states whose representatives participated in exercises organized by the NÚKIB.

Non-technical table-top exercises have repeatedly shown that **staff of key security institutions in the Czech Republic often have low awareness of the nature of cyberspace and cyber security emergencies as such.** It is this lack of knowledge of the functioning of cyberspace, the potential risks and the deeper nature of digital hygiene that often leads to inconsistent compliance. Critical thinking is also needed to properly assess threats and is a key aspect in recognizing phishing attacks or defacement, which today can be very sophisticated and look credible at first glance. Exercises regularly reveal low target audience resistance to manipulations and misinformation, and this is inherently connected with cyber security.

2.

Exercises regularly highlight an absence of strategic communication solutions (also STRATCOM) at national level. The interconnectedness of cyberspace and its actors requires close cooperation and coordination. A cyber incident often harms multiple entitles. In such a situation, coordinating not only the actual resolution of the incident but also communicating it to the public (and potential attackers) is essential. However, the media aspect, which is part of almost all exercises, is not perceived uniformly by the participants. The importance of external communication itself and the question of who should be the responsible coordinator at national level are viewed differently. If an incident affects both private and public institutions, the issue of a single line for external communication becomes all the more difficult.

Strategic communication should be a coordinated effort by the whole public sector that will support the set priorities of the Czech Republic. In the absence of coordination and synergy, it will be difficult to implement such communication and achieve the set priorities.

3.

Cyber security is still often perceived as a specific area that should be covered exclusively by designated institutions. In order to ensure the security in the Czech Republic, it is necessary to move away from the perception of cyber security as purely technical and therefore an issue that can only be addressed by technical staff or specialized institutions. Educated and involved management across government is essential to effectively ensure cyber security and address crises.

Awareness raising and education in the Czech Republic: A long road, but a necessary one

Generally speaking, it is users who, through ignorance or carelessness, make the work of attackers easier. Building habits for the safe use of digital technologies is a core digital literacy competency and deserves due attention. Through consistent awareness rasing and education, undesirable situations and phenomena can be prevented. Education activities in the Czech Republic are quite varied and focus on the most vulnerable population groups, mainly children and seniors.

National cyber security awareness raising and education activities that took place in 2018 included:

E-Safety project:

In 2018 404 events took place within this project. 8,362 children, 579 parents, 983 teachers, 656 various specialists and 73 seniors were trained under the auspices of this project led by Palacký University. The project's online counselling centre handled 334 cases.[xxiii] Two national research projects were also implemented and a professional monograph published. This project won the national round of the European Crime Prevention Award;

Safer Internet Day:

This took place on 6 February 2018 and included a press conference by the National Safer Internet Centre in Prague. Many entities were involved in promoting safety, including the E-safety portal and a number of municipalities and schools;

Say No!:

Europol International Campaign Against Child Abuse Online, held at the Zlín International Film Festival for Children and Youth. The campaign is promoted in the Czech Republic through the Police of the Czech Republic – National Centre for Combating Organised Crime.

Education is a very important variable in terms of the Czech Republic's cyber security. The NÚKIB is therefore involved in working groups that prepare revisions of framework educational programs. In particular, the Agency has sought to integrate cyber security issues more significantly into school education. These efforts have yielded significant results and cyber security is penetrating into education as an integral part of digital literacy. [xxiv] Meanwhile, efforts to promote cyber security education at schools mostly face questions as to whether it is an informatics or cross-discipline topic and whether cyber security education is a matter for educators or parents. Instead of incorporating cyber security into education, schools choose lectures or discussions from external organizations (Czech Police, NGOs, the NÚKIB and others) with the justification that they do not feel confident about the topic or that they lack the necessary knowledge. They also mention the feeling that they have nothing to pass on to pupils in this respect, as pupils have much more experience on the Internet than teachers.

A similar situation exists in the area of media education, the purpose of which is to enhance pupils'

ability to resist disinformation and other similar phenomena. The ability to work with information is also understood by the NÚKIB as an important skill for life in an information society, and which indirectly contributes to ordinary users building a safer cyberspace. It is therefore worth mentioning the survey "State of Media Education in Secondary Schoolsh", [xxv] which shows, for example, that 77% of the interviewed teachers think this is an important area of education, but there is also general uncertainty and disagreement on how to teach and who should teach these topics.

Based on the aforementioned reasons, the NÚKIB has created guideposts for primary [xxvi] and secondary [xxvii] teachers to help teachers orientate themselves in this issue and provide them with support and methodological guidance. The Czech branch of the AFCEA also organizes High School Cyber Security Competitions.

A research report entitled Parent and Parenting in the Digital Era, published by Palacký University in Olomouc and O2 Czech Republic in 2018 provided interesting findings. The report recalls that both schools and **parents play important roles in education regarding the safe use of digital technologies**. One positive finding is that more than half the parents interviewed talk to their children about dating online and 80% of the parents involved in the survey discuss general safety issues relating to Internet communication with their children. [xxviii] The need for parental support is also reflected by the NÚKIB, which last year also prepared a Guide for Parents [xxix] – material to facilitate the upbringing of children in an information society.

In the case of the older generation, i.e. seniors, the state of cyber literacy was revealed by an extensive survey called "Seniors on the Net, [xxx] in which Seznam.cz and Palacký University in Olomouc participated. This research focused on different age groups of seniors and looked at their cyber literacy – for example, how secure their passwords are. One of the findings from this research was that the passwords of more than 50% of those interviewed aged over 55 did not meet general recommendations and could not be considered safe. The NÚKIB has also prepared an appropriate guidepost, [xxxi] for this target group, which reflects some research findings, serves as material for self-education for seniors and provides advice, tips and recommendations for safer use of the Internet.

The education of people working for the **state and public administration** is a priority, as in the exercise of their profession they come into contact and work with a lot of sensitive data. An essential prerequisite for the safe functioning of the state is the adoption of the correct use of digital technologies and work with data. The NÚKIB has therefore launched two **online courses for public administration**.

The first course

The first gives the target group a basic insight into the issue of cyber security. **21,443 civil servants** have successfully passed this course. Of this number, 7,493 were civil servants under the Labour Code and 13,950 civil servants under the Civil Service Act;

The second course

The second reflects the Cyber Security Act. It is intended for people entrusted with the exercise of a security role pursuant to Decree No 82/2018, on Security Measures, Cyber Security Incidents, Reactive Measures and on Determining the Requirements for Filing in the Area of Cyber Security (Decree on Cyber Security). This course was attended by **111 officials**, of whom 57 under the Labour Code and 54 under the Civil Service Act.

Network probes in key state authorities: Early warning of cyber attacks

Cyber attacks are rarely isolated incidents. Single-actor attacks often target multiple institutions simultaneously. In order for the Czech Republic to be better aware of harmful activities in the state's strategic networks, the NÚKIB has implemented a project called "**System for the detection of cyber security events in selected PAIS**"[12]. It aims to make it easier for the administrators of these key state networks to find attackers and better protect those networks by deploying network probes.[13]

Network probes help warn about suspicious data connections, anomalous data volumes leaving a particular network, detect "tapping" of the network from the outside, and serve as an early warning tool for impending 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 be detected by a department or would not be evaluated as dangerous, and allow it to inform other organizations about them before their possible implementation.

At the end of 2018 network probes were deployed by 20 government partners. Local administrators have been properly trained to share cyber security events and selected data about network traffic passing through the network perimeter with GovCERT. GovCERT stores and analyses the received data. Work is currently underway to finetune the system and link it to internal databases and an update server to publish updated threat lists back to the partners involved.

In the future, the project will be further expanded to include other entities which have their own network traffic monitoring. The more entities involved in the project, the more accurately the picture of harmful activities in the Czech institutions will be rendered, and the earlier the warnings about them.

[12] *Public Administration Information Systems*
[13] *The project is not related to plans for the deployment of probes in electronic communications networks by Military Intelligence.*

Election process protection: Czech knowledge also resonates abroad

In light of attacks abroad, the Czech Republic began to review the cyberresistance of its electoral process eight months before the 2017 parliamentary elections. A working group of the Ministry of the Interior was established for the protection of elections and the Czech Statistical Office started close cooperation with the **NÚKIB**. The outcome was a number of measures ranging from mapping the electoral process and analysing its weaknesses, through infrastructure penetration testing to cyber security exercises. The whole process resulted in several recommendations implemented by the CZSO. However, the cyber security of elections is not absolute and it is necessary to work on it constantly.

2017

01

02 **February 2017**

Establishment of the Working Group of the Ministry of the Interior for the Protection of Elections and the beginning of closer bilateral cooperation between the NÚKIB and the CZSO

03 **March 2017**

Beginning of the three-month mapping of the election process. The entire electoral processing chain was examined and potential weaknesses identified based on the analysis

04

05 **May 2017**

Penetration testing of the infrastructure used in the election process

06 **June 2017**

Cyber security exercise organized for the CZSO, based on cases of attacks on elections abroad

07 **July–September 2017**

Recommendations for increasing the cyber security of the election process

08

09

10 **October 2017** (parliamentary elections):

DDoS on the volby.cz and volbyhned.cz websites

2018

01 **January 2018**

Cyber security exercise focused on interactive launches of crisis scenarios

02

03

04 **April 2018**

Meeting of technical experts of the CZSO and the NÚKIB, at which the measures taken so far and the next steps were evaluated

05

Thanks to its experience in securing the electoral process, the Czech Republic, together with Estonia, led the preparation of recommendations for securing the elections to the European Parliament. The result is the freely available “Compendium on Cyber Security of Election Technology”, with over 20 EU Member States involved, as well as the European Commission, the European Network and Information Security Agency (ENISA) and European Parliament representatives.

The Compendium on Cyber Security of Election Technology document is available here:

https://www.govcert.cz/cs/informacni-servis/akce-udalosti/2624-doporuceni-k-zajisteni-kyberneticke-bezpecnosti-volebnich-procesu/

The recommendations that emerged from the document touched upon a number of important areas for secure electronic processing and the announcement of election results. They focused on, for example:

A

The importance of robust anti-DDoS solutions, encryption, real-time network surveillance with SIEM tools, network segmentation, backup and other engineering measures;

B

Problems in penetration testing of electoral systems ranging from the traditional approaches of the Czech Republic and the Netherlands to Estonia, which has published the complete source code and documentation of its election software for several years;

C

The operation of IT election security teams formed of vote-counting organizations, the cyber security authority, and possibly relevant ministries and secret services;

D

Secure software development, including supply chain security;

E

Or risk assessment and crisis management.

F

And the other.

One of the recommendations was to include political parties and their representatives in the security election training. The attacks in the United States (DNC Hack) and France (#MacronLeaks) have clearly shown that cyber attacks often go hand in hand with disinformation campaigns that try to discredit one of the candidates and thus influence the election results. Therefore, political leaders should be mindful of secure communication methods in both their personal and professional life.

FENIX project: Joint protection against DoS and DDoS

As the strength of DDoS attacks increases, so do the demands for protection against them. The Czech Republic became fully aware of this in March 2013, when the country was exposed to a four-day wave of DoS attacks that affected the media, banks and operators, making their websites unavailable. In terms of scope and number of targets, it was the largest cyber campaign the Czech Republic had ever faced.

The FENIX project was created in response to these attacks. It is under the auspices of the NIX.CZ association, which brings together Internet connection and content providers to connect their networks to each other so their customers can communicate quickly.

As regards DoS and DDoS attacks, the purpose of the project is to ensure the availability of Internet services for the entities involved in the project. The FENIX project operates redundant connections and, if one node is overloaded, its operation is automatically redirected to the other connections and availability is maintained. In addition, the project includes other security measures, including:

Monitoring unusually busy connections for project members;

Detection and destruction of amplification attacks (see, for example, Memecached on page 22);

Operation of a surveillance centre that responds within 30 minutes;

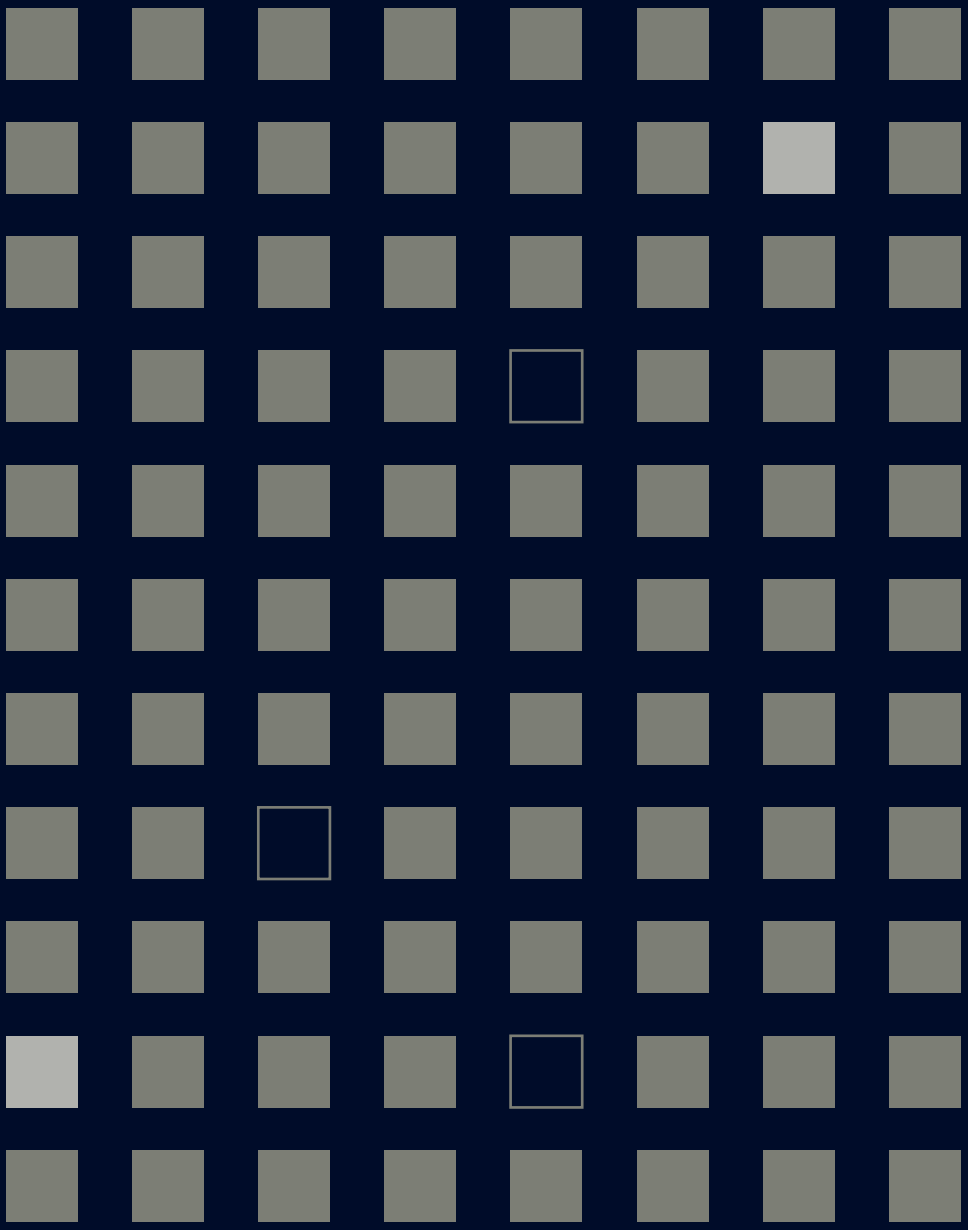
An emergency communication platform;

Contractual prohibition of spam and attacks on the customers of all the project members

Prevention of submitting forged IP addresses in its part of the network (e.g. using BCP-38).

FENIX project members are companies that provide connectivity to major services and need to secure their operations in the most critical situations, meaning the largest Czech Internet service providers are represented in it.

Outlook for 2019



Threats

Cyber espionage

Foreign states' interest in the Czech Republic is very unlikely to fall next year. The activities of state actors in cyberspace related to the Czech Republic will be marked by an increased need to obtain strategic information on the Czech Republic's activities in the EU and NATO, bilateral communication between the Czech Republic and its allies, and bilateral relations. Attacks with the aim of stealing business secrets or intellectual property of Czech companies and research institutions cannot be ruled out, especially in the field of development and research into the new generation of semiconductors, telecommunications technologies, use of satellite technologies, big data processing, artificial intelligence and deep learning.

DDoS

DDoS attacks are likely to continue to grow. The number of unsecured IoT devices increases every year, thereby increasing the numbers of devices that can be incorporated into botnets. Attackers will continue to search for new attack vectors and new ways to increase their effectiveness. Even though organizations are aware of the threats of DDoS attacks and are constantly increasing their resistance to them, they are unlikely to deter attackers altogether.

Data leaks

As databases of personal data offer many possibilities for abuse, it is likely that leaks will continue to increase. Both new leaked databases and previously stolen personal data recycled in newly published compilations will appear. As in previous years, this is very unlikely to avoid the Czech Republic.

Elections

The threat of cyber attacks on elections is likely to continue through 2019. In the spring, Member States will have the European Parliament elections and it will be up to each of them to prepare for them as much as possible. If, as a result of a cyber attack, the results were questioned even in one state, it would not be possible to assign seats to its representatives and the whole electoral process would be compromised. The European Parliament's ability to meet would be impaired, thus affecting the functioning of the European Union as a whole. For states that have long sought to sow distrust of Western institutions, the upcoming European elections must be a tempting target.

Suppliers

The threat of attacks through supply chain weaknesses has been increasing in recent years, and this trend will continue in 2019. Nor can we rule out the detection of older campaigns with subsequent assignment of responsibility to specific groups of actors, including those working for various states. There will also be a trend to update existing regulations to reduce the risk of compromise through supply chains.

Kryptomining

Given the greater effectiveness compared to other types of attacks and the lower risks for the attacker, it is highly likely that attacks using crypto mining will continue in 2019. Existing networks of infected computers (botnets) will probably primarily be used.

Artificial Intelligence and 5G networks

The multiplier for the capabilities of both attackers and defenders will primarily be research and development in artificial intelligence and the expansion of 5G networks. While artificial intelligence will enable actors to automate a large number of complex tasks, fifth-generation networks will be a means for both attackers and defenders to create more massive attack and defence capabilities.

Targets

Public sector:

Attacks on the public sector by foreign states and groups supported by them are highly likely to continue, as are efforts by these actors to operate in public sector networks undetected for as long as possible. However, resilience to such attacks is likely to continue to be negatively affected by a lack of experts and uncompetitive public sector remuneration.

Users:

End users are very likely to remain attackers' primary entry point into their victims' networks. Considering trends abroad, more phishing e-mails can be expected, with the aim of accessing the online interface of Office 365 (Microsoft) and G Suite (Google). Attackers will most likely use fake sites resembling the legitimate login interfaces to retrieve login information. Abroad, the share of phishing messages sent through social networks (Facebook Messenger, Instagram) is also gradually expanding. It is therefore likely that Czech users will also be impacted by this trend.

Energy sector:

The energy sector is likely to be exposed to greater cyber threats next year. The number and sophistication of the attacks will continue to increase, and the deployment of IoT equipment will provide additional scope for possible intrusions into industrial control systems, while attempts to attack through third parties whose networks may not be as secure as the grid and utility networks will increase.

eHealth:

Due to the sensitivity of the data and its attractiveness to attackers, eHealth will remain extremely interesting in 2019. It is likely that the generally decreasing number of ransomware attacks worldwide will mean attacks on eHealth will also decline. On the other hand, we can anticipate an increase in sophisticated, difficult-to-detect attacks on data confidentiality using increasingly sophisticated techniques, especially spear-phishing.

Banking sector:

Attacks on e-banking users are likely to continue in 2019, particularly in the form of attacks on careless mobile phone users.

Academic world:

Phishing campaigns against Czech universities in 2018 show a worrying trend –their number and sophistication increased significantly last year. It is likely that this is just the beginning and that next year the Czech academic sector will remain the focus of cyber actors and that attempts to steal intellectual property will continue.

Annexes

05

Annex 1: Statistics on incidents addressed at GovCERT.CZ

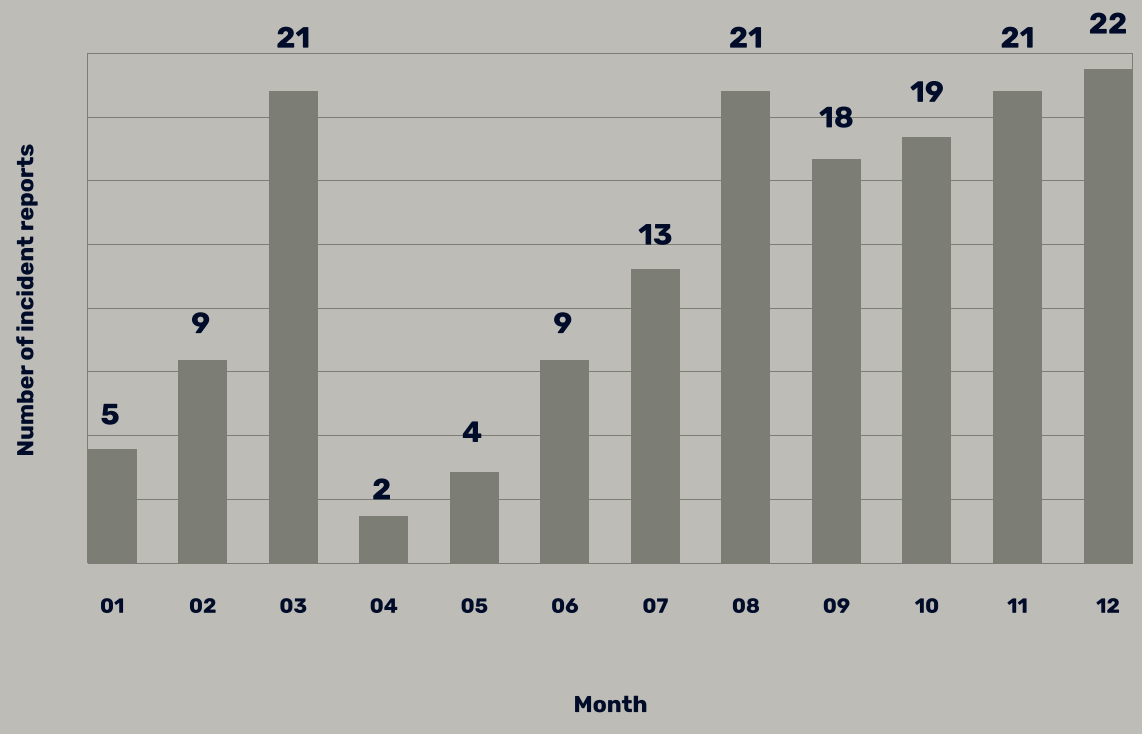
In the course of 2018, GovCERT.CZ employees received 164 relevant reports on cyber security incidents from Czech and foreign partners. These reports were further evaluated as regards the competence of the GovCERT.cz team and subsequently processed either by them or handed over to the relevant entities. In the past year, 54 cyber security incidents falling within the scope of the Government CERT, i.e. CII, VIS and public administration, were evaluated, processed and resolved from the reports received and information obtained by own resources.

Graph 1:

number of incoming reports to GovCERT.CZ concerning incidents in individual months in 2018

Graph 1:

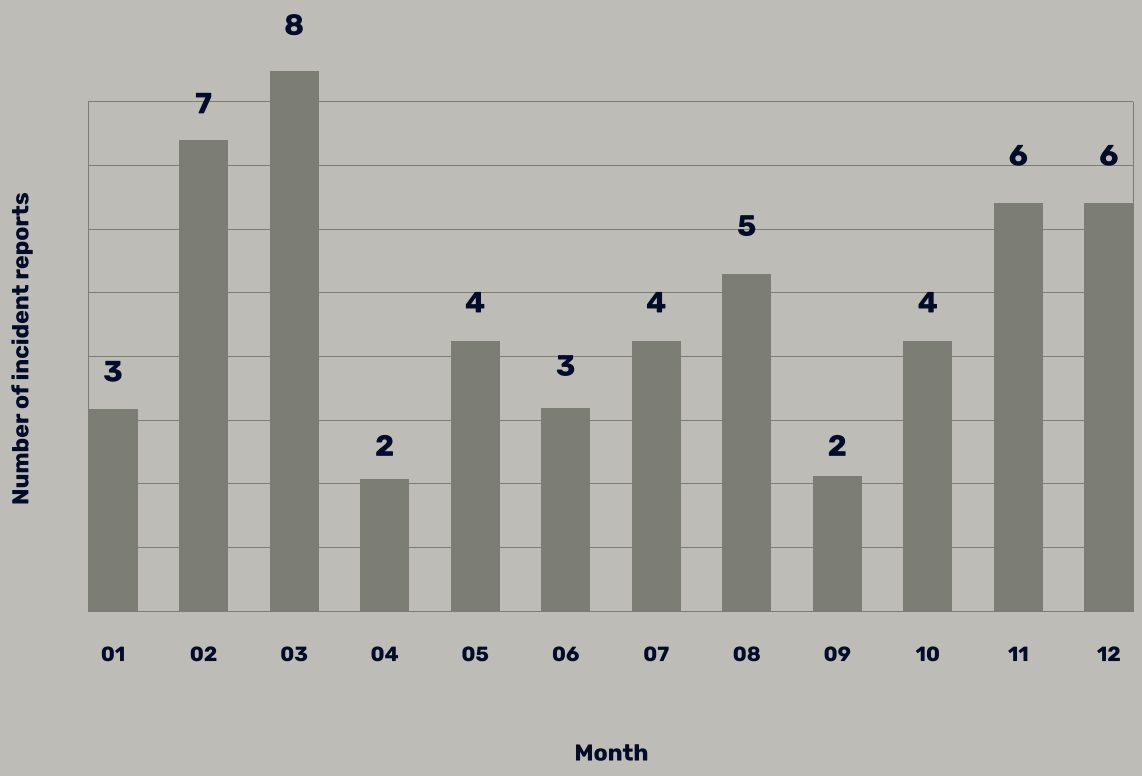
Incoming incident reports in 2018



Graph 2:

number of incidents resolved by GovCERT.CZ
in individual months in 2018

Graph 2:

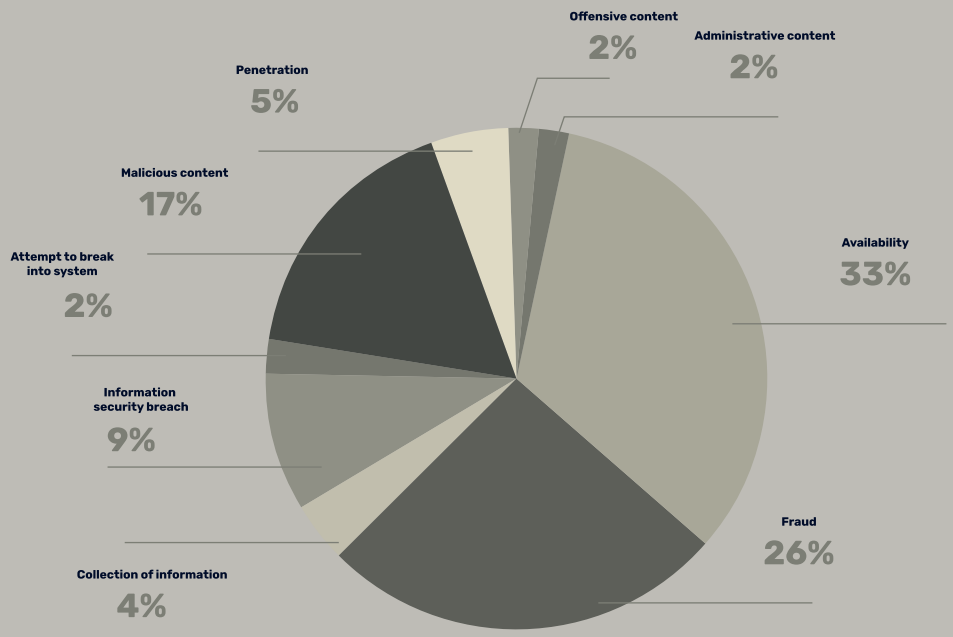


Graph 3:

classification of resolved incidents in 2018

Graph 3:

Classification of incidents in 2018



The category descriptions are based on the incident reporting form:

Offensive content

(such as spam, cyber-bullying, inappropriate content)

Administrative content

(security incident due to administrative error)

Malicious content

(e.g. virus, worm, trojan, dialer, spyware)

Collection of information

(e.g. scanning, sniffing, social engineering)

Attempt to break into a system

(e.g. attempt to exploit a vulnerability, compromise an asset, “0-day” attack)

Penetration

(e.g. successful compromise of an application or user account)

Availability

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

Fraud

Information security breach

Annex 2: How are incidents handled at GovCERT.CZ?

Annex 3: Obliged entities under the Cyber Security Act

Entities obliged to comply with the Cyber Security Act include the following

a) Critical information infrastructure

The protection of critical infrastructure in cyberspace (critical information infrastructure) in the Czech Republic is ensured at legislative level by the Crisis Act and Cyber Security Act. The Cyber Security Act identifies an element or system of elements in this area as critical information infrastructure. This marks a shift from physical objects to information and communication systems. The method for securing these information and communication systems is given by the comprehensive information security management system. The introduction of this system is the central duty that the Cyber Security Act places on obliged entities. Other responsibilities are, for example, reporting contact details, reporting cyber security incidents, and the obligation to carry out measures the NÚKIB may issue

Obliged entities:	Determining procedure:	Implementing legislation:
Manager and operator of a critical information infrastructure information system. Manager and operator of a critical information infrastructure communication system	Critical information infrastructure elements are identified by the NÚKIB by issuing measures of a general nature, or are determined for government departments by a government resolution (the NÚKIB sends a proposal of such elements to the Ministry of the Interior)	Government Regulation No 432/2010 Col., on Criteria for Determining a Critical Infrastructure Element

b) Basic service

The institute of a basic service and its operator was introduced into the Cyber Security Act based on European legislation requirements. Basic service operators primarily differ from Critical Information Infrastructure entities in that in their case the issue is exclusively the securing of the social or economic activities they operate. This stems from the very definition of a basic service, which means a service whose provision is dependent on electronic communications networks or information systems and whose disruption could have an impact on the security of social or economic activities in any of the

sectors listed by law. These sectors overlap with critical information infrastructure sectors in several cases. These sectors are energy, transport, banking, financial market infrastructure, healthcare, water management, digital infrastructure and the chemical industry. The method for ensuring the protection of such systems is then identical with the critical information infrastructure.

Obliged entities:	Determining procedure:	Implementing legislation:
Manager and operator of the basic service information system Basic service operator	NÚKIB shall designate a basic service operator and a basic service information system by issuing a decision	Decree No 437/2017 Coll, on Criteria for Determining an Basic Service Operator

c) Important information system

By definition, an important information system is an information system managed by a public authority and, at the same time, if a breach of information security could limit or significantly jeopardize the exercise of its authority. It is therefore a group which consists exclusively of entities such as ministries and also higher self-governing territorial units or schools, health insurance companies, professional chambers and the like. Unlike critical information infrastructure systems or basic services, these are not determined by the NÚKIB within the framework of important information systems, but it is the duty of each public authority to assess compliance with the criteria and report the identified important information systems.

Obliged entities:	Determining procedure:	Implementing legislation:
Manager and operator of an important information system	The public authority itself will assess the fulfilment of criteria according to Decree No 317/2014 and report to the NÚKIB as an obliged entity; the second possibility is that the information system is included in Annex 1 to Decree No 317/2014	Decree No 317/2014, on Important Information Systems and their Determining Criteria

d) Digital service provider

A digital service is an information society service pursuant to Act No 480/2004, on certain information society services, which consists of operating an online marketplace, an Internet search engine, or cloud computing. However, a digital service provider is not a small enterprise or a micro-enterprise according to Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.

Obliged entities:	Determining procedure:	Implementing legislation:
Digital service provider	The entity itself assesses the fulfilment of the legal definition and reports to the operator of the national CERT as an obliged entity	Commission Implementing Regulation (EU) 2018/151 of 30 January 2018

Annex 4: Report on the state of implementation of the Action Plan on the National Cyber Security Strategy of the Czech Republic for the period 2015 to 2020

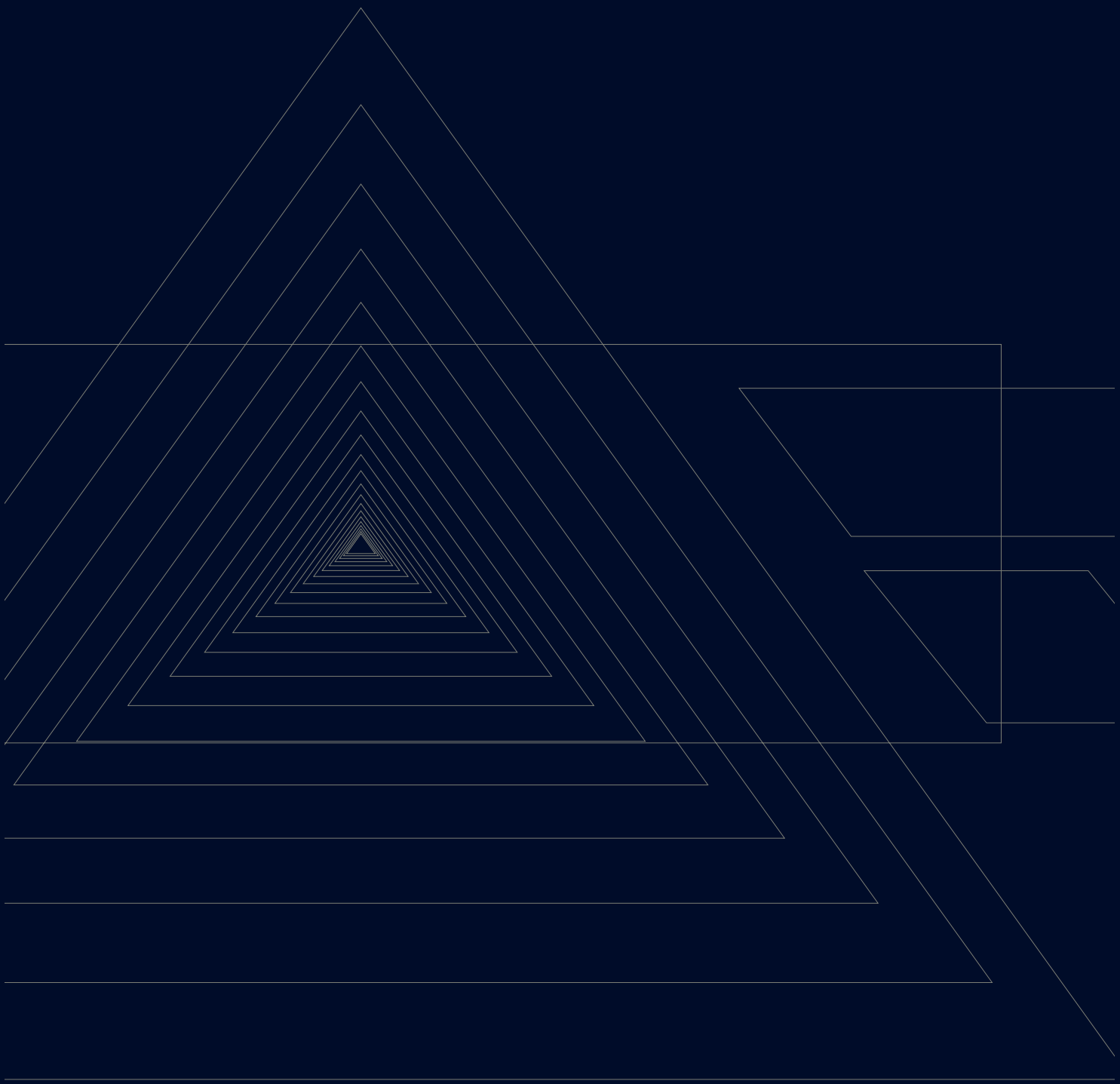
This report is attached as a separate document.

The report reflects the state of fulfilment of the tasks of the Action Plan on the National Cyber Security Strategy of the Czech Republic for the period 2015 to 2020 with a deadline of the fourth quarter of 2018 and tasks to be fulfilled on an ongoing basis. The report will be available on the NÚKIB website.

Probabilistic terms used in the Report on the state of cyber security 2018

Probabilistic terms and the expression of their percentages.

Term	Probability
Almost certainly	90–100 %
Highly likely	75–85 %
Likely	55–70 %
Cannot be excluded / Realistic possibility	25–50 %
Unlikely	15–20 %
Highly unlikely	0–10 %



06 Links

i Pačka, Roman. 2015. Role státu v zajišťování kybernetické bezpečnosti. Bezpečnostní teorie a praxe, č. 3. str. 93–110.

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

iii Sanger, David. 2018. Hacked European Cables Reveal a World of Anxiety About Trump, Russia and Iran. NY Times. https://www.nytimes.com/2018/12/18/us/politics/european-diplomats-cables-hacked.html?smtyp=cur&smid=tw-nytimes

iv Avast. 2018. Top 10Biggest Data Breaches in 2018. https://blog.avast.com/biggest-data-breaches

v Bing, Chrisopher. 2018. Clues in Marriott hack implicate China – sources. Reuters. https://www.reuters.com/article/us-marriott-intnl-cyber-china-exclusive/exclusive-clues-in-marriott-hack-implicate-china-sources-idUSKBN1O504D

vi Hunt, Troy. 2018. Data Provided by the Estonian Central Criminal Police is Now Searchable on Have I Been Pwned. https://www.troyhunt.com/data-provided-by-the-estonian-central-criminal-police-is-now-searchable-on-have-i-been-pwned/

vii iRozhlas. 2018. Loňský útok hackerů při parlamentních volbách? Odloženo. Policie pachatele nevypátrala. https://www.irozhlas.cz/zpravy-domov/cesky-statisticky-urad-hackeri-hackersky-utok-parlamentni-volby-rijen-2017_1805110600_hm

viii Slížek, David. 2019. České ISP na přelomu roku potrápila vlna silných DDoS útoků. Lupa.cz. https://www.lupa.cz/aktuality/ceske-isp-na-prelomu-roku-potrapila-vlna-ddos-utoku/

ix Policie ČR. 2018. Upozornění na výhružné e-maily. https://www.policie.cz/clanek/upozorneni-na-vyhruzne-e-maily.aspx

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

xi Český parlament. 2011. Zákon č. 118/2011 (krizový zákon). http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=22968

xii V překl. National Cyber Security Centre. 2018. Additional information: Russia's malicious cyber activity. https://www.ncsc.gov.uk/content/files/protected_files/article_files/Russian%20State%20Sponsored%20Actor%20Advisory.pdf

xiii National Cyber Security Centre. 2018. APT10 continuing to target UK organisations. https://www.ncsc.gov.uk/news/apt10-continuing-target-uk-organisations

xiv FireEye Intelligence. 2018. TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers. https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html

xv Department of Justice. 2017. U.S. Charges Three Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage. https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations

xvi Národní centru kybernetické bezpečnosti. 2014. Malware Havex útočí na ICS/SCADA systémy. https://www.govcert.cz/cs/informacni-servis/hrozby/2294-malware-havex-utoci-na-icsscada-systemy/

xvii US Department of Homeland Security. 2016. Cyber Attacks Against Ukrainian Critical Infrastructure. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

xviii Eset. 2018. GreyEnergy: Updated arsenal of one of the most dangerous threat actors. https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/

xix Eset. 2017. Industroyer: Biggest threat to industrial control systems since Stuxnet. https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

xx Bundesamt für Sicherheit in der Informationstechnik. 2018. The State of IT Security in Germany 2018. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2018.pdf;jsessionid=91EF3BA2F7D18807A3DD05C6E290343E.2_cid351?__blob=publicationFile&v=3, pg. 12

xxi ESET. 2018. Banking Malware: Sophisticated Trojans vs. FakceBanking Apps. https://www.welivesecurity.com/wp-content/uploads/2019/02/ESET_Android_Banking_Malware.pdf

xxii Polesný, David. 2018. Díra v systému České školní inspekce. Osobní údaje 140 tisíc žáků si mohl kdokoliv stáhnout. Živě.cz. https://www.zive.cz/clanky/ceska-skolni-inspekce-ma-diru-v-systemu-osobni-udaje-140-tisic-zaku-si-muze-kdokoli-stahnout/sc-3-a-195817/default.aspx59

xxiii Centrum prevence rizikové virtuální komunikace PdF UP. 2019. E-Bezpečí v roce 2018. 2019. E-bezpečí. http://www.e-bezpeci.cz/index.php/z-nasi-kuchyne/1415-e-bezpeci-v-roce-2018

xxiv Národní ústav pro vzdělávání. 2019. Návrh revizí ICT. http://www.nuv.cz/file/3362/

xxv Jeden svět na školách. 2018. Stav výuky mediální výchovy na středních školách. https://www.jsns.cz/nove/projekty/medialni-vzdelavani/vyzkumy/6517086_ucitele_medialni_vychovy_celkova_zprava_v24jp.pdf

xxvi Národní úřad pro kybernetickou a informační bezpečnost. 2019. Rozcestník pro učitele základní školy. https://nukib.cz/download/vzdelavani/rozcestniky/Rozcestn%C3%ADk%20pro%20u%C4%8Ditele%20z%C3%A1kladn%C3%AD%20%C5%A1koly.pdf

xxvii Národní úřad pro kybernetickou a informační bezpečnost. 2019. Rozcestník pro učitele střední školy. https://nukib.cz/download/vzdelavani/rozcestniky/Rozcestn%C3%ADk%20pro%20u%C4%8Ditele%20st%C5%99edn%C3%AD%20%C5%A1koly.pdf

xxviii Kopecký, Kamil a Szotkowski, René. 2018. Rodič a rodičovství v digitální éře: Rizikové chování rodičů v on-line prostředí ve vztahu k dětem. E-Bezpečí. https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/107-rodic-a-rodicovstvi-v-digitalni-ere-2018/file

xxix Národní úřad pro kybernetickou a informační bezpečnost. 2019. Rozcestník pro rodiče. https://nukib.cz/download/vzdelavani/rozcestniky/Rozcestn%C3%ADk%20pro%20rodi%C4%8De.pdf

xxx Kopecký, Kamil a Kožíšek, Martin a Szotkowski, René a Kasáčková, Jana. 2018. Starci na netu: Výzkumná zpráva 2018. E-Bezpečí. https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/102-starci-na-netu-2017-2018/file

xxxi Národní úřad pro kybernetickou a informační bezpečnost. 2019. Rozcestník pro seniory. https://nukib.cz/download/vzdelavani/rozcestniky/Rozcestn%C3%ADk%20pro%20seniory.pdf