DOI 10.5817/MUJLT2021-2-7

CYBER SECURITY: LESSONS LEARNED FROM CYBER-ATTACKS ON HOSPITALS IN THE COVID-19 PANDEMIC[1]

by

JAN KOLOUCH[*], TOMÁŠ ZAHRADNICKÝ[**], ADAM KUČÍNSKÝ[***]

The article deals with the issue of cyber security, specifically the security of medical facilities. The introduction summarizes and briefly analyses the cyber-attacks demonstrated on Czech health care facilities in the period from 12/2019 to 1/2021, together with the procedures adopted by the responsible authorities. The article also newly presents the current regulatory requirements for cyber security of hospitals. In the context of past attacks and based on analysis of attacks, current legislation and events, the article will provide an opinion on whether the requirements for cyber security of hospitals are set sufficiently or whether this area should be revised. At the same time, measures will be recommended to strengthen the cyber security of hospitals.

KEY WORDS

Critical Infrastructure Protection, Legal Framework, Cyber Security, Cyber-attack, CSIRT, CERT, Healthcare

[1] This article was supported by the European Regional Development Fund "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01/0.0/0.0/16_019/0000822).

[*] jan.kolouch@cesnet.cz, CESNET a.l.e., Prague; jan.kolouch@law.muni.cz, CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence (C4e), MUNI, Brno.

[**] tomas.zahradnicky@vse.cz; Department of Systems Analysis, Faculty of Informatics and Statistics, Prague University of Economics and Business, Prague.

[***] a.kucinsky@nukib.cz; Department of Cybersecurity Regulation, the National Cyber and Information Security Agency, Brno.

1. INTRODUCTION

The article provides a summary of significant publicly known cyber-attacks on Czech hospitals that occurred in the period from 12/2019 to 1/2021. This period is also significant that due to the SARS-CoV-2 virus pandemic (hereinafter referred to as "COVID-19"), hospitals, or rather medical facilities, are subject to significantly higher requirements than in the normal period. There are problems with the capacity of medical facilities and the staffing shortage in these facilities. Capacity is often compensated by temporary changes in hospital structures and restrictions on non-acute care, while staffing shortages are partially offset typically by the services of volunteers and medical students called etc.

Following the analysis of cyber-attacks from the above period, the reaction of stakeholders in the field of cyber security will be described. The procedure of the National Cyber Information Security Agency (hereinafter also "NCISA") will be described, as well as the regulatory requirements for cyber security of hospitals and their changes since the beginning of 2021.

In the context of cyber attacks conducted at the healthcare sector in the Czech Republic, the article will provide a framework and recommendations for improving the legal and technical aspects of cyber security in that sector. Based on this framework, it will be possible to verify whether the existing cyber security requirements for healthcare facilities are sufficiently set. Another output of the article will be information on whether the area of cyber security in the healthcare sector should be revised, and if so, proposals for specific adjustments will be made. At the end of the article, recommendations and proposals of measures that can help strengthen the cyber security of medical facilities will be presented.

Based on the Czech Republic's approach to healthcare cyber security, recent law changes, and authors' own analysis, the authors demonstrate possible risks and pitfalls implementing a minimal cybersecurity standard and legislation in other countries.

2. SIGNIFICANT CYBER SECURITY INCIDENTS IN THE HEALTHCARE SECTOR IN THE CZECH REPUBLIC

Cyber-attacks on medical facilities are not a new problem. In the USA, the first cyber-attacks on these facilities combining phishing and ransomware appeared already in 2016.[2] Outside the USA, there have been cases of attacks in many other countries, including the Czech Republic. Since December 2019, the Czech Republic has been affected by cyber-attacks at ICT infrastructure of numerous medical facilities, some of which have crippled their normal operation for up to several weeks and caused extensive damage.

Medical facilities are currently heavily dependent on ICT infrastructure. In practice, this has shown, among other things, that medical facilities are currently unable to function fully without ICT infrastructure and provide services for which they are primarily established. The dysfunction or unavailability of information and communication technologies and services related to them can, in extreme cases, endanger the lives of patients[3]. Such a strong dependence on ICT infrastructure poses a significant risk.

The risk of the successful attack can often be minimized by organizational and technical measures after analysis of previous attacks.

Based on a detailed analysis of the cyber-attack performed on 11th December 2019 at the Rudolph and Stephanie Regional Hospital in Benešov (HBEN), which we presented in the article Cyber Attacks on Czech Hospitals in the Covid-19 Pandemic[4], we analyzed other similar attacks carried out on the territory of the Czech Republic at the time when a state of emergency was declared on the basis of the COVID-19 pandemic for a significant part of the year. The attacks and their resolution will be studied, and an opinion will be offered on whether the current regulatory requirements are sufficient or whether they should be amended and if so how.

The following table provides a chronological listing of significant publicly known cyber-attacks targeting medical facilities in the Czech Republic between 12/2019 and 1/2021. The table is presented to demonstrate ransomware attacks in healthcare in a relatively short time frame during the COVID-19 pandemic.

[2] *Ransomware: See the 14 hospitals attacked so far in 2016*. [online] Available from: https://www.healthcareitnews.com/slideshow/ransomware-see-hospitals-hit-2016?page=1 [Accessed 10 May 2017] also: *Three US hospitals hit by ransomware*. [online] Available from: https://www.bbc.com/news/technology-35880610 [Accessed 10 May 2017].

[3] Deutsche Welle (2020). *German police probe 'negligent homicide' in hospital cyberattack*. [online] Available from: https://p.dw.com/p/3ieQl [Accessed 19 February 2020].

[4] Kolouch, J., Zahradnický T. and Kučínský A. (2021) *Cyber Attacks on Czech Hospitals in the Covid-19 Pandemic.* Unpublished manuscript.

Target of the Attack	**Detection**	**Malware**	**Impact**	**Damages Est.**
The Rudolph and Stephanie´s Regional Hospital in Benešov (444 beds)	11. 12. 2019	Emotet TrickBot Ryuk	Decommissioning Malfunction of some ICT services	CZK 59 million
University hospital Brno (1889 beds)	12. 3. 2020	Defray777	Decommissioning Unavailability of patient data.	Hundreds of milion of CZK
The Psychiatric hospital in Kosmonosy (600 beds)	27. 3. 2020	Dewar	Encryption of shared storage, domain and application disks. Loss of part of the backups.	Unknown
The Hospital for long-term illnesses in Horažďovice (140 beds)	January 2020	Buran	Unauthorized use, damage and deletion of data.	CZK 150 000

Table 1: An overview of successful publicly known attacks at Czech hospitals in 2019-2021

For the purposes of this article, especially for the purpose of introducing a minimal security standard (cf. Section 7), we have decided to briefly summarize each of the attacks from the technical point of view.

The Rudolf and Stefanie's Hospital in Benešov (HBEN). In the case of the attack on HBEN, the Microsoft office document containing macros was opened after the initial phishing email. A user overrode the warning by hitting the "Enable Content" button, the malicious macro within the document executed further executing a PowerShell script which in turn downloaded the Emotet trojan from the Internet, running it, and starting off the first stage of the infection. There are other possibilities for Emotet installation such as running a stand-alone infected script or by downloading its executable directly by accessing a malicious link in e-mail. TrickBot was used to conduct reconnaissance and to ultimately deliver Ryuk (ransomware). Ryuk is a common final payload for banking Trojans (like TrickBot). Research from SonicWall[5] claims that Ryuk represented a third of all ransomware attacks so far in 2020.

The University Hospital in Brno (HBRNO) was infected with the Defray777 malware. The Defray malware family first appeared in 2017, targeting the Education and Health Care sector[6] and since then has undergone a number of modifications. The most widely occurring infection with Defray777 today comprises of launching Vatet Loader, performing Cobalt Strike attack, and ultimately deploying Defray777. The attack begins with a phishing e-mail with an attachment in the form of a Microsoft Office document containing an embedded OLE Packager Object. According to Trend Micro[7], phishing emails are now well-crafted — for an attack targeting a hospital, the phishing email was from a "hospital IT manager" and the malicious files were disguised as patient reports. If the victim clicks on the OLE file, the attack was initiated launching the Vatet Loader[8]. The Vatet Loader launches the Cobalt Strike attack to perform reconnaissance and spread laterally over the network and to provide remote access to the network. Once the malware operator decides, the attack ends by deploying Defray777. After running Defray777, the listed processes will end, and data encryption will begin. Data on local disks and attached network storage is encrypted by a combination of AES and RSA algorithms. The decryption key for the AES cipher is encrypted by the RSA algorithm

[5] Wadhwani, S. (2020) *Cyber World's Most Fearsome Ransomware Is Ryuk: SonicWall*. [online] Available from: https://www.toolbox.com/security/threat-reports/news/cyber-worlds-most-fearsome-ransomware-is-ryuk-sonicwall/. [Accessed 19 February 2020].

[6] Proofpoint, Inc. (2020) *New Defray Ransomware Targets Education and Healthcare Verticals*. [online] Available from: https://www.proofpoint.com/us/blog/threat-insight/new-defray-ransomware-targets-education-and-health-care-verticals. [Accessed 19 February 2020].

[7] Trend Micro Incorporated (2017) *Defray Ransomware Sets Sights on Healthcare and Other* Industries. [online] Available from: https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/defray-ransomware-sets-sights-on-healthcare-and-other-industries. [Accessed 19 February 2020].

[8] Tracey, R. and Schmitt, D. (2020) *When Threat Actors Fly Under the Radar: Vatet, PyXie and Defray777*. [online] Available from: https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/. [Accessed 19 February 2020].

and sent to the control server under the control of the attacker. After the encryption is completed, the user is asked to pay a ransom for decrypting his data.

The Psychiatric Hospital in Kosmonosy (HKOS). The attack began again with a phishing campaign, this time to launch the Dewar ransomware. This ransomware belongs to a group of malware called Phobos[9]. The initial infection can occur through the insecure Remote Desktop port[10] or through phishing. In the case of phishing, Dewar is distributed as e-mail attachments containing, for example, executable files, archives, Microsoft Office files and PDF documents, or javascript code. After the initial infection, lateral spreading occurs, for which operators can use a variety of methods. The infection ends with a ransom notice after all document files are encrypted. The effects of Dewar ransomware are very similar to those of Defray777.

The Hospital for long-term illnesses in Horažďovice (HHOR). This hospital was attacked by Buran ransomware, which is a development of the older VegaLocker ransomware. Buran[11] spreads through phishing, a publicly accessible Remote Desktop interface, and through the vulnerability of the out-of-date Microsoft Internet Explorer. After it runs and ensures the persistence in the Microsoft Windows operating system registries, privilege escalation tools such as Mimikatz[12] may run to obtain administrator-level access. With administrator privileges, operational logs are deleted, the Windows Event Log service is turned off, and restore points and any local backups are deleted. Finally, the encryption of user data on local disks and attached network storage is started while the decryption key is sent to the control server. Finally, the user is left with a file with ransom requests for decrypting his data. Fortunately, there was no massive spread of this malware at the hospital.

[9] Elshinbary, A. (2020) *Deep Analysis of Ryuk Ransomware*. [online] Available from: https://n1ght-w0lf.github.io/malware%20analysis/ryuk-ransomware/. [Accessed 19 February 2020].

[10] *Ibidem.*

[11] Mundo, A. (2019) *Buran Ransomware; the Evolution of VegaLocker*. [online] Available from: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/buran-ransomware-the-evolution-of-vegalocker/. [Accessed 19 February 2020]. Sette, N. (2020) *Malware Analysis – Buran Ransomware-as-a-Service*. [online] Available from: https://www.kroll.com/en/insights/publications/cyber/malware-analysis-buran-ransomware-as-a-service. [Accessed 19 February 2020].

[12] Delpy, B. and Le Toux, V. (2020) *Mimikatz*. [online] Available from: https://github.com/gentilkiwi/mimi-katz/releases. [Accessed 19 February 2020].

All of the above-mentioned attacks have a common factor which is the usage of phishing and ransomware. However, this is not a new, unknown and as yet unpublished phenomenon. Examples include historically older sources – ransomware attacks Defray (years 2016 and 2017)[13], WannaCry (2017)[14], etc.

Given the relatively well-known "modus operandi" of attackers (ie. the use of phishing campaigns and ransomware), the relatively high success rate of their own attacks is surprising. On the other hand, it should be borne in mind that the medical facilities, and in particular the staff of these facilities at the time of the COVID-19 pandemic, are primarily involved in recovering and rescuing as many patients as possible and their caution in relation to phishing e-mails and defective attachments is reduced, among other things, due to mental and physical exhaustion. Another factor increasing the success of these attacks is the way in which temporary staff is recruited in a state of emergency in the form of volunteering and work duty[15]. Employees recruited in this way pose a significant risk, as they may have access to the ICT of the healthcare facility, but they do not always have sufficient computer security habits.

When we compare the presented ransomware attacks to similar attacks in other countries, the average downtime of 15 days and the breadth of damage[16] applied to the Czech attacks as well.

This section summarized publicly known attacks using a combination of phishing and ransomware in the Czech Republic between 9/2019 and 1/2021. This is not an isolated problem and hundreds of similar attacks have already taken place on the world stage. Furthermore, the success of pandemic attacks is increasing due to the strain that causes users to lose vigilance when opening malicious attachments, as well as the potentially insufficient training of temporary staff. In addition to the hospitals

[13] Trend Micro Incorporated (2017) *Defray Ransomware Sets Sights on Healthcare and Other Industries*. [online] Available from: https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/defray-ransomware-sets-sights-on-healthcare-and-other-industries. [Accessed 19 February 2020].

[14] Landi, H. (2019) *Report: 40% of healthcare organizations hit by WannaCry in past 6 months*. [online] Available from: https://www.fiercehealthcare.com/tech/lingering-impacts-from-wannacry-40-healthcare-organizations-suf-fered-from-attack-past-6-months. [Accessed 19 February 2020].

[15] In case of crisis resolution, most countries have a possibility to summon physical persons for work duty for necessarily long time. In the Czech Republic, the work duty institute is defined in article 2 (d) of the Act No. 240/2000 Coll., On Crisis Management.

[16] Davis, J. (2020) *Ransomware Causes 15 Days of EHR Downtime, as Payments Avg $111K*. [online] Available from: https://healthitsecurity.com/news/ransomware-causes-15-days-of-ehr-downtime-as-payments-avg-111k. [Accessed 19 February 2020].

themselves, law enforcement agencies and anti-virus companies, the National Cyber and Information Security Agency (hereinafter referred to as "NCISA") also participated in resolving the impacts of the cyber security incidents described above.

3. NCISA'S ROLE IN CYBER INCIDENT HANDLING

After a brief analysis of significant cyber-attacks on medical facilities, we will describe how NCISA was involved in solving not only the cyber security incidents described above. It is the central administrative body for cyber security, including the protection of classified information in the field of information and communication systems and cryptographic protection[17]. As a regulator, NCISA determines and enforces the fulfillment of obligations in the field of cyber security of defined bodies and persons, and at the same time has the capacity to resolve cyber security incidents, especially through its organizational unit, which is the Government CERT (Computer Emergency Response Team).

NCISA actively participated in resolving incidents targeting the health sector in 2019 and 2020. Both HBEN and HBRNO had the staff directly at the scene of the incident. At the same time, in response to the attacks and their secondary threat, they did the following:

1. issued a reactive measure in March 2020[18],
2. in April 2020, they issued a warning[19] against attacks on organizations in the Czech Republic, especially hospitals.

Reactive Measure (RM) is a measure defined within article 13 (1) of Act No. 181/2014 Coll., On Cyber Security (hereinafter referred to as "ACS"). According to this article "*NCISA issues a decision ordering to take reactive measures to deal with a cyber security incident or to secure information systems or electronic communications networks and services from the cyber security incident, which is the first act in a case.*" RM is a measure the state can issue to involve state bodies into a cyber-attack resolution. From the EU legislative perspective, the Directive (EU) 2016/1148

[17] The National Cyber and Information Security Agency (2021) *About NÚKIB*. [online] Available from: https://www.nukib.cz/en/about-nukib/. [Accessed 19 February 2020].

[18] The National Cyber and Information Security Agency (2020) *NCISA issued a reactive measure for select health care subjects*. [online] Available from: https://www.nukib.cz/cs/infoservis/aktuality/1418-nukib-vydal-reaktivni-opatreni-pro-vybrane-subjekty-ve-zdravotnictvi/. [Accessed 19 February 2020].

[19] The National Cyber and Information Security Agency (2020) *Cyberattack threat at the hospitals and other significant targets in the Czech Republic.* https://www.nukib.cz/cs/infoservis/aktuality/1425-hrozba-kybernetic-kych-utoku-na-nemocnice-a-jine-vyznamne-cile-cr/. [Accessed 19 February 2020].

Of European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (hereinafter referred to as "NIS") states that "*digital service providers should be subject to light-touch and reactive ex post supervisory activities justified by the nature of their services and operations*."[20] The NIS directive also states in article 8 (5) that member States shall ensure that the competent authorities have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of the NIS directive.

If we compare the possibilities declared by the NIS directive and the ACS to national authorities, we must conclude that the ACS empowers NCISA with much more proactive capacity to handle some cyber incidents than is required by the NIS directive. In our opinion, the Czech legislation can be an inspiration for other states as well, especially in the case when the revision of the NIS directive is being prepared.

The issuance of the reactive measure is an act by which NCISA can order selected addressees to do something and/or refrain from doing so. This is to increase the security of the systems, and thus prevent or resolve a cyber security incident. From the point of view of resolving a security incident, this is the reactive power of NCISA, which can, with this institute, correct the security of information or communication systems if the condition of response to the incident is met. It should be added that NCISA may issue such a measure only in relation to those systems and entities affected by the Cyber Security Act, and the administrators of these systems are then obliged to notify the NCISA of the implementation of the measure and the manner of its implementation.[21]

Reactive measures may be issued on the general basis by measures of the general nature or by the decision pursuant to the Administrative Procedure Code. A measure of the general nature is issued if the number of addressees is not limited or not specified[22] and takes effect immediately by posting on the official notice board of NCISA[23]. Its efficiency is therefore significantly accelerated compared to the standard state. The decision according to the Administrative Procedure Code is addressed to a specific administrator(s) of critical information infrastructure systems, essential

[20] Recital 60 NIS.

[21] Article 13 (4) ACS.

[22] Article 13 (3) ACS.

[23] Article 15 ACS.

service, or a significant information system. The fact that this authorization of NCISA is to respond to acute threats or incidents is emphasized by the fact that the appeal filed against the decision has no suspensive effect.

Reactive measures responding to attacks on medical facilities were issued on 17th March 2020 and were addressed to those medical facilities that fall under the ACS as operators of the essential service. In the conditions of the Czech Republic, there were a total of 16 medical facilities.

The reason for issuing this specific reactive measure was both the attacks on HBEN and HBRNO and the effort to minimize the risk of similar incidents in the future, i.e. securing ICT systems against cyber security incidents.

The reactive measure in question required the addressees to perform a total of 20 specific actions divided into 4 sets according to the time frame for their fulfillment. At the same time, it contained the legitimacy of non--performance of any of the acts, in such a way that the act is not necessary to perform if its performance would cause a greater impact than the incident itself. A methodology was issued for the reactive measure, which specified it, stated the objectives of individual actions and recommendations for their implementation. The content of the reactive measure can be described as follows:

1. *without delay:*

Avoid interconnection of systems except when necessary. Interconnection between systems allows an attacker from one system to access another system. For each connection, it is therefore necessary to consider whether it is absolutely necessary and, if not, not to allow such a connection at all. We assume that all connections are a-priori prohibited and whitelisting, not blacklisting techniques, are employed to allow connections only when necessary and always to the smallest possible extent.

Avoid communication to the Internet except when necessary. If a system can communicate to the Internet without restrictions, an attacker can download data to/from it and/or attack it from anywhere if it is directly accessible from the Internet. It is therefore advisable to use restrictive firewall settings and not allow outgoing communication to the Internet. If the system already needs to communicate to the Internet, such as some modalities, it is appropriate to use egress filtering (i.e. outbound filtering) and allow access only to a whitelisted set of IP addresses.

Separate the network of medical devices from the rest of the network. Specialized medical devices (modalities) often need to communicate to the Internet. However, these modalities may be obsolete, without new updates, and therefore vulnerable. Such devices must be isolated from the rest of the medical device's network by being allocated to a separate network segment. A more suitable solution seems to be to create one isolated network segment for each modality. Furthermore, it is appropriate not to allow communication in between the modality network(s) and other networks except for the absolutely necessary individual cases, which will be determined by whitelisting.

Change the passwords of privileged accounts. The password change was forced due to the installation of malware on the computer system. As such, malware could intercept, among other things, already used user's passwords. A privileged account allows access to and control of critical systems. This account allows to bypass standard security mechanisms and manipulate sensitive data stored in ICT systems and applications. These are usually administrator accounts for software and hardware operated within the organization, administration scripts, user and application accounts, accounts for social networks, etc.

Report to the NCISA the current IP ranges. The aim of this action is usually to obtain data to facilitate the investigation of the incident and possible further attacks. At the same time, ranges are an important source of data for checking whether they are not present in the investigated malicious communication. NCISA can also perform vulnerability scans and provide other services upon request. Therefore, it is necessary to report a list of both public IPv4 and IPv6 address ranges.

2. *within 2 days:*

Move backups offline and check the functionality of backups. If the backup is offline, it cannot be attacked by a remote attacker with a ransomware attack. Therefore, it is important to have at least part of the backups offline. It is also important to verify that the recovery from the backup works correctly.

Do not delete data on cyber security incidents. Most hardware and software record data about their activities in operational records (logs). For example, logs can contain IP addresses, usernames, timestamps, and other information that may be important in resolving cyber security incidents. This data should have sufficient retention so that it can be used to obtain more detailed information in the event of an incident.

Check sent indicators of compromise. NCISA sends compromise indicators (IOC) to selected subjects. These most often take the form of IP addresses, the occurrence of which should be checked in the operational records. If an IOC address appears in the records, it cannot be ruled out that one of the systems has been compromised and further steps need to be taken to verify the potential attack.

Alert employees to the risk of phishing. Phishing is very sophisticated today, so it is necessary to periodically train and check employees. Phishing does not have to take the form of a fake, trusted-looking e-mail that is written in good Czech, for example from a supervisor. These can be, for example, lost keys with the hospital logo and a USB stick on which the malware is located. Bare insertion of the stick into a computer can start off the infection. Therefore, it is necessary to periodically train and test employees so that they do not open unknown attachments, connect unknown devices to the computer, and do not share any login details (social engineering) with anyone. In case of suspicion and finding of the device or an attempt to obtain login information, for example by phone, employees should be trained to contact a designated employee.

3. *within a week:*

Verify that backups are separated so that even a privileged administrator cannot delete them. An attacker could use software tools to gain the access to a privileged administrator account, as well as the right to delete any file, including backups. Therefore, you must verify that even the highest-privileged account does not have permission to delete and/or overwrite backups. This can usually be solved by using local accounts instead of accounts located in the Active Directory.

Disable the use of unsigned macros if possible. Much of the malware spreads through infected Microsoft Office documents and takes the form of macros. They can be enabled by the user to start the first phase of the infection. Macros can be digitally signed with the private key to the Microsoft Authenticode digital code signing certificate, making them trusted. To prevent random users from running unsigned macros, it is a good idea to disable this organization-wide through the Administrative

Templates files and the Office Customization Tool for Microsoft 365 Apps and Enterprise, Office 2019, and Office 2016 in the Active Directory domain.

Check network segmentation and control between segments. Proper network segmentation and well-set segment interconnection rules can greatly reduce the impact of ransomware infection. The network should therefore be divided into segments, with intersegment communication being a priori denied. Only communication that is necessary and to the least extent possible should be allowed by whitelisting.

Tighten endpoint security policies (ban on running unapproved applications, unsigned PowerShell, etc.). The Microsoft Windows operating system allows you to list applications that the user can run through Group Policy in the form of whitelisting. It is also advisable to disable unsigned scripts for Microsoft PowerShell on this system. Whitelisting of running applications also offers other operating systems, and especially on mobile devices that connect to the LAN (tablets and mobile phones), this is important because these devices are often neglected.

If business continuity management is not implemented – develop business continuity plans at least for key systems. Business continuity management allows you to foresee potential threats and provides plans for their solution. There should be offline plans for key systems that can be used in the event that the system becomes infected with malware and becomes unavailable.

Perform a vulnerability scan in systems accessible from outside the organization. NCISA offered to perform the scan. A periodic scanning of vulnerabilities on public IP addresses allows the organization to verify that unwanted services are not exposed to the Internet, and that systems are properly updated and do not contain known vulnerabilities.

4. *within 2 weeks:*

Deploy antivirus on all relevant devices. Deployment of an antivirus solution on all relevant devices, including client stations, file and mail servers. Antivirus and antimalware software is a necessary security layer today and is not the domain of the Microsoft Windows operating system alone.

Consider deploying updates after testing them. Deploying system updates can be problematic in an enterprise environment due to concerns about breaking system functionality by applying a patch. Nevertheless, it is important to prioritize security patches.

Note that patches can be tested before deployment. Whether a patch should break something, if it is not available, or if it cannot be applied, it is important to consider isolating the non-patched system from the surrounding network.

At the time of the issuance of the reactive measure, it is necessary to consider as essential or critical steps those that have the shortest time interval given for their fulfillment.

In this context, the change of passwords of privileged accounts (measures responding to the situation in the already compromised network), prevention of network interconnection and disconnection of unnecessary services from access to the Internet (measures against possible attacks) can be emphasized.

The section described the role of NCISA in solving cyber security incidents. It described how the reactive measure was being issued, including the specific steps taken by NCISA in response to the HBEN incident. The framework of the actions of the reactive measure issued on 17th March 2020 was also presented. In the next section we will summarize long-term recommendations for dealing with ransomware attacks and compare them with the recommendations of the US Cyber security & Infrastructure Security Agency and its warning AA 0-302 A[24].

4. LONG-TERM RECOMMENDATIONS FOR HANDLING RANSOMWARE ATTACKS IN THE HEALTHCARE SECTOR

In the long run, ensuring cyber security is a range of individual measures that are often mutually supportive and interlinked. If we limit ourselves to measures responding to ransomware attacks, it is necessary to recommend at least from the above-mentioned and detailed measures:

Regular staff training. The attackers focus on the weakest point in the organization. The weakest point means usually people, i.e. users and administrators. It is important to constantly increase security awareness through introductory and periodic training. To maintain awareness and vigilance, it is also advisable to conduct testing, for example, through internal phishing campaigns, which can both verify the effectiveness of security training and keep users alert.

[24] Cybersecurity & Infrastructure Security Agency (2020) *Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector* [online] Available from: https://us-cert.cisa.gov/ncas/alerts/aa20-302a. [Accessed 19 February 2020].

Significant network segmentation. Network segmentation is a key measure to limit the spread and thus the amount of data affected in the event of a ransomware attack. Network segmentation allows to include, for example, classic users or modalities into various segments. Modalities have a much longer lifetime than traditional ICT equipment and often run on platforms that are no longer supported. If network segmentation is missing, an attacker can move virtually unrestricted in the organization, causing much larger damage. Individual segments can then have differently set permissions and options for where they connect and who accesses them[25].

Minimize the use of administrator accounts. The use of privileged accounts should be restricted on the basis of the principle of minimum privileges. Thus, privileged rights should be granted only to those who absolutely need them, and at the same time privileged accounts should be used only when absolutely necessary. The need to grant a privileged authorization to each specific account should be assessed periodically and, if the condition of necessity ceases, the authorization should be revoked. If the privileged account is compromised by ransomware, a significantly greater amount of damage can be expected.

Backup, regularly test backups, keep backups offline. Backup is a basic and effective measure against the effects of ransomware. Backing up your organization's data from ransomware may not protect it, but it can repair the damage. Backups work if done correctly. NCISA recommends the following backup rules:

- Rule 3 – 2 – 1 = At least 3 copies on 2 different devices, of which 1 outside the organization.
- Inactive backup = At least one or more backups shall be inactive (offline) at one time. Consistently deploy identity management and access control for cloud backups.
- Recoverability and recovery plan = Backups shall be tested and usable for recovery.

Regularity and existence of a backup plan = Backups shall be created regularly[26].

Have business continuity plans (BCMs) and test them. Even the best security is not 100% guarantee that an incident will not occur. In addition

[25] Donovan, F. (2019) *How Network Segregation, Segmentation Can Stop Ransomware Attacks.* [online] https://hitinfrastructure.com/features/how-network-segregation-and-segmentation-can-stop-ransomware-attacks. [Accessed 19 February 2020].

to preventive measures, it is also necessary to think about reactive measures. In particular, it is necessary to have a functional recovery plan, which will clearly define the individual systems and their prioritization with regard to the impact on the achievement of organizational goals, deadlines and responsibilities for individual actions and, last but not least, procedures for system recovery. It is advisable to test these plans regularly to ensure that they are up-to-date, functional and usable in a crisis situation. Requirements for continuity plans can be found, for example, in the Cyber Security Ordinance or in IEC/ISO 22301[27].

Regularly check applications accessible from the Internet and evaluate whether they are still necessary. Organizations often have services open to the Internet. It is completely logical, because through these services, users, administrators or suppliers can access the ICT environment. Attackers can try to break into these services and gain access to the system. It also happens that organizations have historical services open to the Internet, which administrators do not know or maintain for various reasons. These services become vulnerable and very dangerous because they can be used by attackers to break into the organization.

For comparison, we present a set of recommendations issued by the Cyber security & Infrastructure Security Agency (hereinafter referred to as "CISA"). Within the Alert (AA 0-302A) on Ransomware Activity Targeting the Healthcare and Public Health Sector[28], as an immediate response to a similar type of attack as in the Czech Republic, the recommendations were divided into levels:

- Network infrastructures
    - Patch operating systems, software, and firmware as soon as manufacturers release updates.
    - Check configuration for every operating system version for HPH organization-owned assets to prevent issues from arising

[26] The National Cyber and Information Security Agency (2020) *Ransomware: Recommendations* for Mitigation, Prevention, and Reaction. [online] Available from: https://www.nukib.cz/download/publikace/pod-purne_materialy/Ransomware%20-%20Doporuceni_pro_mitigaci_prevenci_a_reakci.pdf. [Accessed 19 February 2020].

[27] European Union Agency for Cybersecurity (2020) *Procurement Guidelines for Cybersecurity in Hospitals*. [online] Available from: https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services. [Accessed 19 February 2020].

[28] Cybersecurity & Infrastructure Security Agency (2020) *Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector* [online] Available from: https://us-cert.cisa.gov/ncas/alerts/aa20-302a. [Accessed 19 February 2020].

    that local users are unable to fix due to having local administration disabled.
  - Regularly change passwords to network systems and accounts and avoid reusing passwords for different accounts.
  - Use multi-factor authentication where possible.
  - Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
  - Implement application and remote access allow listing to only allow systems to execute programs known and permitted by the established security policy.
  - Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
  - Audit logs to ensure new accounts are legitimate.
  - Scan for open or listening ports and mediate those that are not needed.
  - Identify critical assets such as patient database servers, medical records, and telehealth and telework infrastructure; create backups of these systems and house the backups offline from the network.
  - Implement network segmentation. Sensitive data should not reside on the same server and network segment as the email environment.
  - Set antivirus and anti-malware solutions to automatically update; conduct regular scans.
- Ransomware Best Practices
  - Regularly back up data, air gap, and passwords protect backup copies offline.
  - Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, secure location.
- User Awareness Best Practices
  - Focus on end user awareness and training about ransomware and phishing.
  - Ensure that employees know who to contact when they see suspicious activity or when they believe they have been a victim

of a cyberattack. This will ensure that the proper established mitigation strategy can be employed quickly and efficiently[29].

If we compare the content of the reactive measure with the recommendations of NCISA and CISA, we come to a strong agreement. However, as it turns out, despite high-quality recommendations in the field of cyber security, which aim to reduce the risk of security incidents caused by ransomware attacks, these recommendations are not mandatory, except for actions of reactive measures for entities within the scope of the ACS. The following section will discuss how NCISA can proceed in the prevention of incidents in the healthcare sector.

5. NCISA'S CYBER ATTACK PREVENTION POSSIBILITIES IN THE HEALTHCARE SECTOR

Reactive measures as they are defined by the ACS cannot be applied to organizations that do not fall within the scope of the ACS[30]. Due to the fact that the ACS, and thus also reactive measures, covers only a small part of the total number of medical facilities (only 16 medical facilities in the Czech Republic fell under the ACS in 2020, as they were operators of essential service according to Article 3 (g) ACS), in response to cyber-attacks, NCISA was forced to issue recommendations for health service providers supplemented by a methodology.

16th April 2020, NCISA issued, in accordance with Section 12[31] of the ACS,

> *"Cyber Security Threat Warning, consisting in the implementation of a large-scale campaign for serious cyber-attacks on information and communication systems in the Czech Republic, especially medical systems[32]."*

[29] Cybersecurity & Infrastructure Security Agency (2020) *Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector.* [online] Available from: https://us-cert.cisa.gov/ncas/alerts/aa20-302a. [Accessed 19 February 2020].

[30] Adressees of the reactive measure are obliged subjects defined in Article 3 ACS.

[31] The institute of warnings is defined in Section 12 of the ACS as an act to be issued by the NCISA if it *"learns in particular from its own activities or at the initiative of the national CERT operator or from bodies performing activities in the field of cyber security abroad about the threat in cyber security."*

[32] The National Cyber and Information Security Agency (2020) *Cyberattack threat at the hospitals and other significant targets in the Czech Republic.* https://www.nukib.cz/cs/infoservis/aktuality/1425-hrozba-kybernetickych-utoku-na-nemocnice-a-jine-vyznamne-cile-cr/. [Accessed 19 February 2020].

The warning is published on the NCISA website and sent to obliged subjects in accordance with the law[33].

NCISA's own findings and warnings from partners led to the issuance of a warning dated 16th April 2020, and this information raised legitimate concerns about the real threat of serious cyber-attacks on important targets in the Czech Republic, but above all on medical facility systems.

The threat of these attacks was classified as high, i.e. grade three on the four-point scale used by the NCISA. Such a threat is therefore probable to very probable (51-75%)[34].

As such, an alert does not directly impose rights or obligations, but defines the threat and its severity. Entities falling under the ACS must work with this threat and take it into account in their own risk analysis. The entities concerned must respond to these risks by applying appropriate and proportionate organizational and technical measures[35].

In the issued warning, the Agency also recommended that the following actions be taken:

- Warn users against spear phishing.
- Prevent macros from running in Microsoft Office products.
- Block unnecessary access from the external Internet to the hospital's network infrastructure.
- Implement offline backups including checks of their functionality.

The warning itself was further supplemented by a recommendation, which included other actions to increase the security of organizations[36].

This warning expired on 20th May 2020. According to the justification,

> *"the probability of the threat that was the subject of the warning decreased, i.e. intensity of the threat for which the warning was issued was reduced. [37]"*

[33] Article 12 (2) of the ACS.

[34] NCISA uses a 4-point threat severity scale. This scale is also used in the Cybersecurity Decree, Annex 2. Threat severity is evaluated as: 1 – low, threat does not exist or has low probability (probability 0-25 %), 2 – medium, threat is low probable to probable (26-50 %), 3 – high, threat is probable to highly probable (51-75 %), 4 – critical, threat is highly probable to more or less certain.

[35] The National Cyber and Information Security Agency (2020) *Supplementary materials*. [online] Available from: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/. [Accessed 19 February 2020].

[36] The National Cyber and Information Security Agency (2020) *Recommended security measures to warning from 16th April 2020. Supplementary material.* [online] Available from: https://www.nukib.cz/down-load/uredni_deska/Doporuceni_k_varovani_2020-04-17.pdf. [Accessed 19 February 2020].

[37] Article 6 justification to end a warning, https://www.nukib.cz/cs/uredni-deska/.

This section stated the possibilities of NCISA in the field of prevention of cyber security incidents. Unfortunately, even the warning does not impose any obligation to take any action, so the following section will analyze the regulatory requirements in the field of cyber security in the health sector to propose adjustments that would increase the number of entities covered by ACS and further enforce a minimum-security level for this sector.

6. APPLICABLE LEGAL FRAMEWORK IN THE CYBER SECURITY WITHIN THE HEALTHCARE SECTOR

The aim of this chapter is to present the regulatory framework of cyber security and its specific impact on the health sector.

At the EU law level, we can observe ongoing significant changes based on awareness of the cyber security attack risks and insufficient security of key systems of individual member states. The security enhancement of personal data and medical data can be observed in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR). Beside GDPR, the cybersecurity area was also codified in the NIS directive, which states that the magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union.[38]

The NIS directive defines in article 4 an *operator of essential services* term. A subject is an *operator of essential services* if it meets criteria laid down in Article 5 (2) of the NIS directive.

According to the NIS directive, the following is required to the essential service and to the health sector particularly:

> *„in addition to the cross-sectoral factors, sector-specific factors should also be considered in order to determine whether an incident would have a significant disruptive effect on the provision of an essential service. With*

[38] *DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. [online] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN. [Accessed 20 February 2020].

> *regard to health sector, it could be the number of patients under the provider's care per year, provided services etc. "*[39]

The Czech Republic implemented the requirements from the NIS draft into the ACS yet in 2014, that is 2 years before the NIS directive came into effect. Based on the experience NCISA earned since the ACS came into effect and increasing number of attacks, it was necessary to amend the ACS and the underlying decrees several times, including criteria for determination of the operator of essential service in health care. The experience also helps adjusting a minimal legislative standard for these operators not only in the Czech Republic, but also in other member states or during the NIS revision process.

ACS regulates:

> *"the rights and obligations of persons and the competence and powers of public authorities in the field of cyber security, incorporates the relevant regulations of the European Union and regulates the security of electronic communications networks and information systems.* [40]"

The ACS does not affect all users of cyberspace, but only the entities listed in Article 3 ACS. Regarding the determination of whether a medical facility falls under the competence of the ACS, the obligatory subjects according to Article 3 (c), (d), and (f). Particularly speaking about:

(c) an operator and an administrator of a critical information infrastructure information system,

(d) an operator and an administrator of a critical information infrastructure communication system,

(f) an operator and an administrator of an information system of essential service, unless they are the operator, or the administrator specified in letters c) or d).

Ad c) and d)

Critical information infrastructure is Article 2 (b) ACS defined as an element or system of elements of critical infrastructure in the field of communication and information systems in the field of cyber security.[41]

Critical infrastructure (hereinafter also "CI") and thus also critical information infrastructure (hereinafter also "CII") is determined according

[39] Recital 28 NIS.

[40] Article 7 ACS justification to end a warning, https://www.nukib.cz/cs/uredni-deska/.

to cross-sectional and sectoral criteria in the field of cyber security in Article 2 (i), Crisis Act and further in Government Order No. 432/2010 Coll. on the Criteria for the Identification of a Critical Infrastructure Element (hereinafter also "OCID").

According to the OCID, it is a necessary precondition for the inclusion of a medical facility in a critical infrastructure that such a facility has at least 2,500 acute beds.

However, there are no medical facilities that meet this condition in the Czech Republic, and therefore, according to the current legal framework, no medical facility can be included in CI.

Regarding the connection to the CII, it is necessary to assess the fulfillment of the criteria in the sector: VI. Communication and information systems, part G – Cyber security. Five criteria are defined here, which state that a critical information infrastructure can be identified:

a) an information system which significantly or fully influences the activity of an identified element of critical infrastructure, and which is at the same time replaceable only if excessive costs are incurred or in a time period of more than 8 hours,

b) a communication system which significantly or fully influences the activity of an identified element of critical infrastructure, and which is at the same replaceable only if excessive costs are incurred or in a time period of more than 8 hours,

c) an information system which is operated by a public authority that execute public powers which contains personal data of more than 300,000 people,

d) a communication system securing the connection or interconnection of an element of critical infrastructure, with a capacity of guaranteed data transmission of at least 1 Gbit/s,

e) sectoral criteria for the identification of a critical infrastructure element specified in A to F shall be used adequately for the field of cyber security, if the protection of the element fulfilling these criteria is necessary to ensure cyber security.

If we study the criteria in more detail, we will find that the first two criteria allow to determine as CII only those systems that affect the specified

[41] The very concept of critical infrastructure is defined by Act No. 240/2000 Coll., On Crisis Management (Crisis Act), which states "*that it is a complex of elements (in our case, information and communication systems), the disruption of which could have a serious impact on security of the state, provision of the basic living needs of the population, health of persons or the economy of the state.*" See article 2 (g) Crisis Act.

element of CI, while medical facilities do not meet this condition. Of the other criteria, it is possible to apply only the criterion listed under letter e) to medical facilities, but the fulfillment of this criterion is relatively difficult to assess in reality, and it is also proven due to its uncertainty and vagueness. In addition to the sectoral criteria, NCISA must prove the fulfillment of cross-cutting criteria in the process of assessing the inclusion of a certain entity in the CII. This can be difficult in the context of healthcare facilities, as there is no inclination in healthcare legislation. It is thus difficult to prove how many potential patients will be affected by the failure of a particular medical facility. However, proving the fulfillment of cross-sectional criteria is a necessary condition for identifying hospitals and their systems as CII. At the same time, there is currently no satisfactory key in the form of sectoral criteria for identifying major healthcare facilities.

Cross-sectional criteria are an important filter for determining CII and are defined in Article 1 of the OCID. When learning an element of a critical information infrastructure, any disruption of this system must be able to cause:

a) more than 250 casualties or more than 2,500 people who needed hospitalization for longer than 24 hours,
b) economic impact with threshold value of economic loss greater than 0.5 % of GDP or,
c) impact on society with threshold value of a large limitation of necessary service provision or another serious intervention into the daily life of more than 125,000 people.

The sectoral criteria of the government regulation for determining CIs are in sector IV. Healthcare, by the Ministry of Health set up so that no medical facility meets them. From the authors' point of view, it would be logical to set these criteria to cover at least the most important players in the industry.

In this case, it is necessary to agree with the conclusions of Harasta, which he states

> *"If we state that the purpose of the legislation is to protect critical infrastructure effectively and efficiently, the current Czech legal development suggests that our statement might be wrong and misguided. The law on its operative level does not sufficiently reflect the broad definition*

> *on a strategic level. Cross-cutting and sectoral criteria allow us to approach certain interdependencies selectively, but not to cover them exhaustively. The broad definition of critical infrastructure as present within legal framework of EU and, as demonstrated on the case of the Czech Republic, in its member states, furthers the securitization of the issue by labeling it as influential enough to move into the realm of law and to achieve institutionalization within its framework. Since the strategic level with its broad definitions has a purpose, simplistic lower-level norms are justified to a certain extent, because they allow for administration in the issue. Therefore, a legal framework of critical infrastructure protection does not present a significant legal value that needs to be maintained – it merely mirrors the lax or active role this issue plays within policy discussions*[42]*."*

Ad f)

Operators of essential services (OES) represent another group of obligated persons according to the ACS, under which possible medical facilities could be included. Operators of essential services represent a group of obliged subjects that were included in the ACS by a transposition amendment to the Act in 2017. This group of liable persons is determined by NCISA pursuant to Decree No. 437/2017 Coll. on the criteria for the determination of an operator of essential service (hereinafter also "DCRIT").

These criteria were defined by the DCRIT, until 31st December 2020, as follows:

a) a total of at least 800 acute care beds in the last three calendar years or

b) the status of a facility for highly specialized trauma care according to the Act on Health Services.

These special criteria for the type of entity represent the importance of the entity in the industry in terms of the size and scope of the services provided. As of 31st December 2020, only 16 medical facilities in the Czech Republic met these criteria.

In the light of the incidents described in the previous chapter, NCISA proceeded to amend the DCRIT, specifically the special criteria of the types of entity. The aim of this change was to expand the number of hospitals that

[42] Harašta, J. (2018) *Legally critical: Defining critical infrastructure in an interconnected world*. International Journal of Critical Infrastructure Protection, vol. 21, pp. 47-56. Elsevier. ISSN 1874-5482.

could be included under the ACS as OES. The criteria are therefore as follows from 1st January 2021 (changes compared to the previous version are marked in bold):

a) the total number of acute beds in the last three calendar years is at least 400, the status of a center of highly specialized traumatological, oncological, cerebrovascular, cardiovascular, complex cardiovascular or perinatological care according to the Act on Health Services,

b) provision of emergency admission according to the Act on Ambulance Service in facilities with a total number of intensive care beds in the last three calendar years of at least 40 or

c) an acute inpatient care provider with an average number of uniquely treated patients in the last three calendar years of at least 100 000 per calendar year.[43]

If at least one of the above special criteria meets the type of medical facility entity, its systems may be assessed in relation to the fulfillment of the impact criteria, which are set at Decree No. 437/2017 Coll., Annex, Sector 5. Health Care.[44]

As healthcare facilities are the controllers of a significant amount of personal data of a special category and data on health status, it is offered to meet at least criterion VI.

As of 31st December 2020, only 16 medical facilities were covered by the ACS, and only these facilities had to introduce safety measures pursuant to Sections 4 and 5 of the ACS, i.e. report contact details[45]

[43] Decree No. 437/2017 Coll., Annex 1, Sector 5. Health Care.

[44] Those criteria are:

The impact of a cyber security incident in an information system or electronic communications network on the operation of which the provision of a service depends may cause:

I. a serious limitation of the type of service which would affect more than 50,000 people,

II. a serious limitation or disruption of another essential service or a limitation or disruption of a critical infrastructure element,

III. unavailability of the type of service for more than 1,600 people which is irreplaceable in another way unless excessive costs were to be incurred,

IV. more than 100 casualties or 1,000 injured people in need of medical treatment or,

V. disruption of public safety in a significant part of the administrative territory of a municipality with extended powers, which may require rescue and liquidation operations by the integrated rescue system units, or

disclosure of sensitive data of more than 200,000 people.

[45] Providing contact information, and therefore a possibility to contact an organization, is an elementary condition for a timely warning and reaction to an imminent cyber-attack. As well as fast notification. Under current conditions, notifications and other measures in the health care sector are only enforceable with difficulties or not at all.

pursuant to Section 16 or comply with measures pursuant to Section 11 of the ACS. It should be added that the organization will be designated as an OES by a decision in administrative proceedings issued by NCISA. Thus, the mere fulfillment of the criteria does not in itself mean the obligation to follow the law immediately.

There are currently at least 232 health care providers in the Czech Republic – medical facilities with inpatient care. We list at least 232, because this number fluctuates more than usual due to the pandemic. The number of 232 was determined on the basis of information from open data published on the website of the National Register of Health Data Providers for the period 1st January 2021 – 31st January 2021[46].

Filtering according to the "*FormaPece*" (type of health care service) field was applied to the data for the occurrence of the word "*lůžková*" (accute beds) and at the same time the "*DruhZarizeni*" (facility type) field for the occurrence of the word "*nemocnice*". The number of 232 medical facilities does not include long-term care hospitals. The numbers of beds were subsequently added to the data and obtained manually from the websites of medical facilities and their annual reports. It was possible to find bed capacity online only in 153 of them.

Due to the fact that all large medical facilities have been reliably added to the list, the data insufficiency is reflected only in smaller medical facilities for which the status of operator of essential service (OES) is not assumed. Medical facilities were further divided according to their bed capacity into bins of 50 beds and the numbers of hospitals in individual bins were determined. The values of the bins were cumulatively summed from 2500 beds to zero.

The following graph shows the cumulative totals obtained indicating the number of hospitals that would meet the OES criterion if set to the number of acute beds equal to the interval of their bin. Thus, it is possible to enter in the graph the minimum number of beds that are codified in law, i.e. 2500 beds for CI, 800 beds for the OES up to and including year 2020 and 400 beds from year 2021 on. Codified values are highlighted in the graph. The gaps in between the columns in the graph were shrunk to conserve space and mean that no data was available for the given interval.

[46] *Národní registr poskytovatelů zdravotních služeb*. [online] Available from: https://opendata.mzcr.cz/data/nrpzs/narodni-registr-poskytovatelu-zdravotnich-sluzeb.csv. [Accessed 20 February 2020].

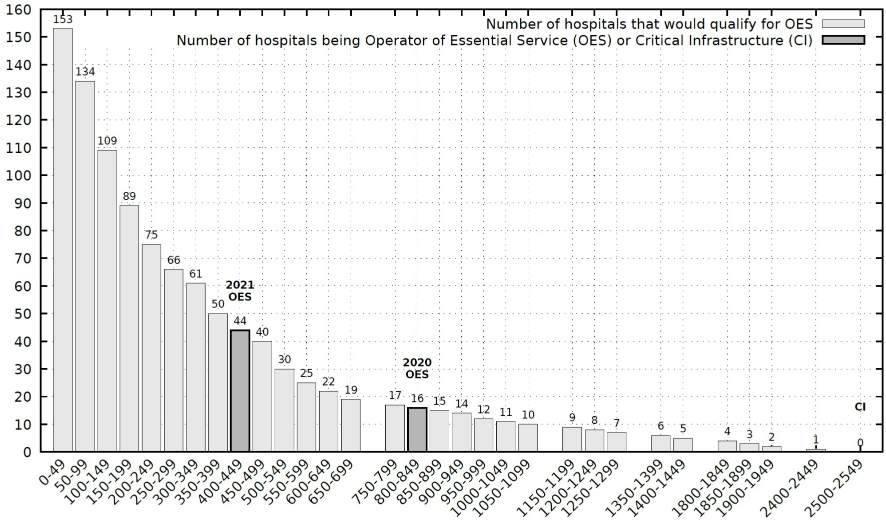

Figure 1. Cumulated number of hospitals that would qualify as operators of essential services (OES). According to the law when setting the criterion – the number of acute beds – to any number of beds from the interval under the x axis. The OES criterion was originally set to 800 beds until the end of the year 2020 and this, according to the figure above, means that there were 16 hospitals with 800 or more beds. From 1st January 2021 on the value was set to 400 beds meaning there will be an estimated total of 44 hospitals falling into the OES.

The data also revealed that adjustments to the minimum number of acute care beds from 800 to 400 beds have now included HBEN among the essential service operators with their 444 beds.

In terms of content, the issued recommendation was very similar to the reactive measure itself (see Chapter 2), but points that are not relevant for non-obligated persons were omitted (for example, the obligation to report its IP ranges to NCISA).

It is clear that NCISA, as the central administrative body for cyber security, wanted to warn other potential victims in response to the described cyber-attacks and the high level of risk of repeating these attacks. For this reason, the recommendation was issued and distributed on 18th March 2020, i.e. immediately after the issuance of the reactive measure[47].

[47] The National Cyber and Information Security Agency (2020) *NCISA issued a reactive measure for select health care subjects*. [online] Available from: https://www.nukib.cz/cs/infoservis/aktuality/1418-nukib-vydal-reaktivni-opatreni-pro-vybrane-subjekty-ve-zdravotnictvi/. [Accessed 19 February 2020].

The recommendation from NCISA as a means of legal coercion of another entity is non-binding and was sent to 85 medical facilities. These 85 medical facilities were designated by the Ministry of Health as the backbone.

This section presented an analysis of regulatory requirements in the field of cyber security for health care providers and provided a graph estimating the number of health care facilities (primary care providers) depending on the minimum number of acute beds. Based on the application of legislative requirements and analysis of available data, it was found that none of the medical facilities in the Czech Republic is part of the critical infrastructure because it does not meet the minimum number of acute beds at 2,500, although one of the hospitals is close to this limit.

It was further stated that until 31st December 2020, only 16 health care facilities met the criterion of a primary care provider and that this criterion was reduced to 400 as from 1st January 2021. Finally, a graph was presented estimating the number of health care facilities among providers of essential services with an accuracy of 50 beds.

The number of medical facilities falling under the ACS since 1st January 2021 has not yet been published, but we can estimate from the graph that there will be approximately 44 medical facilities.

The next part of the article will deal with proposals for amendments to legislation that could further contribute to the cyber security of medical facilities.

7. LEGISLATIVE MEASURES NECESSARY TO INCREASE THE CYBER SECURITY OF MEDICAL FACILITIES

If we summarize the incidents described in the first chapter of this text in terms of ICT implications, it can be stated that the confidentiality, integrity or availability of these systems may be compromised, and thus, for example, complete system control, unavailability, data theft or unauthorized modification. No data theft was detected in the attack cases described above. However, there may also be inaccessibility of information, services and malfunctions of specialized facilities, which has actually happened. The effects of a successful ransomware attack on an affected organization are often fatal in such cases. The organization ceases to function, physical damage to property can occur, and in the case of hospitals, life and health can also be endangered. The reputational and financial implications are almost certain.

A successful attack is not out of the question even with the best preventive measures, and therefore the existence of business continuity plans is absolutely crucial for minimizing the impact of attacks and rapid recovery. From the above-described attacks i tis clear that the disruption of information systems of medical facilities has real consequences. In the Czech Republic these facilities fall under the ACS only to a very limited extent and there is no uniform and enforceable security standard for medical facilities and their ICT systems. Also, no functional communication platform has been created by Ministry of Health that could quickly, accurately and intelligibly inform about cyber-attacks outside the ACS system.

The NCISA's competences are strictly defined by the ACS.

The measures and recommendations summarized above were all meant with good intention, yet they may be difficult to implement.

After analysis of the cyber security incidents at Czech hospitals occurring during the COVID-19 pandemic and discussion with medical care cyber security experts that were unaffected by the attack, we have to conclude that there is no "collective intelligence". There is no platform on which health care providers (and other sectors) could share data on collectively, to learn from, and to acquire and apply experiences of others.

As an appropriate collective intelligence solution, authors propose to create a cyber-attack information coordinator, perhaps per sector, within NCISA or the National CSIRT team. It is a question whether these organizations are understood as a trustworthy partner for the hospitals and other sector organizations, as trust can be built by active approach to share data about attacks and by presentation of appropriate measures[48].

Despite the following text may seem highly technical, authors believe that the depth is necessary for proper definition of minimal security standards in healthcare as a key element for ensuring cyber security in the sector.

On the other hand, it can be stated that the state or territorial self-governing units should also play an important role in the protection

[48] Kolouch, J., Zahradnický T. and Kučínský A. (2021) *Cyber Attacks on Czech Hospitals in the Covid-19 Pandemic.* Unpublished manuscript.

of medical facilities. The state and its bodies are entitled to do only what is expressly permitted by law. For this reason, it was necessary to adjust the legislative framework of these powers in at least the following areas:

- **Amendment of Decree No. 432/2017 Coll. so that more medical facilities are included in the category of operators of essential services (OES)**

By changing the criteria set out in this Decree for operators of basic healthcare services, it is relatively easy to increase the number of healthcare facilities included in the ACS system. NCISA, just in response to the described attacks, has already amended this decree.

According to the available information, the described change allows for the inclusion of another 30 health care facilities in the OES system, i.e. a total of 46 health care facilities could be the operator of basic services in the health care sector.

It is therefore possible to assess whether NCISA has set the change in regulation sufficiently and whether the newly set criteria for determining the operators of basic services are adequate (see the analysis in Chapter 5).

The special criteria for the type of entity for the determination of OES in the healthcare sector are newly established as follows:

a) a total of at least 400 acute care beds in the last three calendar years,

The criterion is basically the same as in the previous version of the decree, but the number of acute beds is reduced from 800 to 400.

b) the status of a facility for highly specialized traumatological, oncological, cerebrovascular, cardiovascular, complex cardiovascular or perinatological care according to the Act on Health Services,

Compared to the previous version of the decree, there is an expansion of medical disciplines in this criterion, when in the original version only one type of center of highly specialized care was mentioned, namely trauma care.

In the Czech Republic, the status of a highly specialized care center is granted in a total of 14 medical fields[49], of which a total of 6 are in the area of cyber security regulation.

[49] A list of centres of highly specialized care in The Czech Republic – Ministry of Health of The Czech Republic.

This extension, in contrast to the original trauma care only, can be described as a step in the right direction, as it will cover other key medical disciplines and services for patients.

c) provision of emergency admission according to the Act on Ambulance Service in a facility with a total number of intensive care beds in the last three calendar years of at least 40,

This is a completely new criterion, which was not in the original version of the decree. This criterion is intended to cover medical facilities to which the emergency medical service is linked. Urgent income is regulated by Act No. 374/2011 Coll., On the ambulance service, which stipulates that it means:

> *"a specialized workplace of a provider of acute inpatient care with continuous operation, which ensures the receipt and provision of intensive acute inpatient care and specialized outpatient care to patients with sudden serious damage to health and to life-threatening patients.* [50]"

The regulation is now also focused on those medical facilities where the emergency medical service primarily transports patients with acute problems.

Acute care is defined by Act No. 372/2011 Coll., On health services and as a type of health care, the aim of which is to

> *"avert a serious deterioration in health or reduce the risk of a serious deterioration in health so that the facts necessary to determine or change individual treatment or that the patient does not end up in a condition that endangers himself or his surroundings*[51]*."*

In-patient care is then divided by the same law into acute in-patient care, intensive care and acute standard inpatient care[52]. The criterion thus takes into account the performance of the hospital, resp. the importance of the hospital in relation to the number of patients treated.

[50] Article 6 (3) Z ZZS.

[51] Černý, V. (2020). *Dostupnost intenzivní péče pro hospitalizované pacienty s COVID-19*. [online] Available from: https://www.uzis.cz/res/file/covid/20200324-cerny-cz.pdf. [Accessed 19 February 2020].

[52] Article 9 (2a, 2b) Act No. 372/2011 Coll.

The total number of medical facilities with resuscitation and intensive acute care (ARO + ICU) in the Czech Republic is 136[53]. The number of ARO beds is 823 and the number of ICU beds is 3658.

d) an acute inpatient care provider with an average number of uniquely treated patients in the last three calendar years of at least 100 000 per calendar year.

This is a completely new criterion, which was not in the original version of the decree. The aim is to include in the regulation those healthcare facilities that provide their services to a large number of patients and are therefore important for the industry in terms of the range of services provided.

- **Amendment of Government Regulation No. 432/2010 Coll. so that more medical facilities are included in the Critical Infrastructure of the state**

As mentioned above, no medical facility is and cannot be presently included in the critical infrastructure of the state.

The authors believe that setting unsatisfiable criteria does not make sense and it would be appropriate to adjust them so that the most important medical facilities fall into the CI.

For example, inspiration can be found in the version of Decree No. 437/2017 Coll., Effective between 1 February 2018 and 31 December 2020:

By lowering the criterion of 2,500 acute beds to 800 acute beds and/or the status of a trauma center, it would be possible to achieve the 16 largest medical facilities as critical infrastructure.

For the regulation of cyber security of medical facilities, resp. their inclusion under the ACS would not be a problem, because according to the principle of "higher regulation takes precedence" (expressed in Article 3 (f) ACS), such an organization could be determined as CII and reassigned into this group from the OES group. This measure would include the inclusion of some medical facilities in crisis management of the country, the possibility of emergency supplies and, in general, better emergency readiness.

- **Setting a minimum-security standard for medical facilities**

The inclusion of selected medical facilities in the regulation of the ACS as one of the obliged subjects is one of the steps to increase the protection

[53] Černý, V. (2020). *Dostupnost intenzivní péče pro hospitalizované pacienty s COVID-19*. [online] Available from: https://www.uzis.cz/res/file/covid/20200324-cerny-cz.pdf. [Accessed 19 February 2020].

of these facilities against cyber-attacks. However, due to the number, diversity and different nature of medical facilities, such regulation will not and can never cover all facilities. Meeting some ACS requirements is not realistic or effective for some health care providers (for instance, due to their size).

Nevertheless, we believe that at least the basic security of medical facilities should be taken into account. It would therefore be appropriate to set a certain minimum-security standard for medical facilities in the field of cyber security. Such a standard should be relatively simple, general given the diversity of organizations, and at the same time binding so as to ensure its widespread application.

To achieve these goals, the following basic questions need to be answered:

a) Who should define the standard?

In order to create an ideal security standard, it would be appropriate to create a working group composed of representatives of regulators, i.e. NCISA and the Ministry of Health, medical facilities, especially those to whom the standard would be addressed.

It would also be appropriate to invite representatives of security forces and the professional public to the working group (e.g. National CSIRTs, auditors operating in the healthcare sector, representatives of anti-virus companies, internet connection providers, etc.).

b) What should the standard contain?

There are a number of security standards and various methodologies for their implementation. In order to determine what a standard should contain; it is appropriate to start in particular from the person for whom such a standard is intended.

The target group of this standard is healthcare providers (especially small and medium-sized hospitals). Such organizations cannot be overwhelmed by complex analyzes that they will not be able to carry out on their own. Nor can they be given a complex management system that they will not be able to apply effectively.

The measures should therefore be simple and cover the underlying risks.

If an organization wants to devote more effort to security, it can always use the regulations on cyber security, the deployment of ISMS according to ISO 27001 or similar standards.

The Minimum Safety Standard issued by NCISA, MI and NAKIT in the middle of 2020 can serve as a basic material from which it would be possible to start, and which could be tailored to the working group by medical facilities.

> *"This document offers simplified principles, procedures and recommendations in the field of cyber security for organizations that do not fall under the regulation of Act No. 181/2014 Coll., on cyber security*[54]*."*

Its development and modification for the environment of medical facilities is thus directly offered.

Standard, resp. the areas and measures it should cover are also described in Chapter 2 of this article. The standard should be divided in terms of risk minimization measures into two parts – organizational and technical.

The organizational part should cover the area:

- classification of information;
- planning the implementation of security measures;
- building security awareness;
- supplier management;
- change management;
- continuity management;
- cyber security control and audit.

The technical part should cover technical safety measures in at least the following areas:

- physical security;
- control of access to information systems;
- network segmentation;
- protection against malicious code;
- cryptography;
- backup;
- protection of web applications;
- security of cloud services.

When defining measures, it must be assumed that individual organizations have different ICT architectures and therefore measures should be defined in general with possible examples of application and the standard should be technology neutral.

[54] The National Cyber and Information Security Agency (2020) *Supplementary materials*. [online] Available from: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/. [Accessed 19 February 2020].

a) What should be a suitable carrier, or on what basis should it be required and enforced?

In order to increase cyber security and the resilience of the health sector as a whole, a minimum-security standard should be mandatory. If this is not the case, cyber security cannot be expected to be considered a priority by healthcare management. In addition, as mentioned above, a minimum-security standard for non-ACS organizations exists and can be deployed voluntarily.

If the minimum-security standard were not mandatory, in the opinion of the authors, a significant improvement of the situation cannot be expected.

As obligations can be imposed in the Czech Republic on the basis of and within the limits of the law, it is necessary that the obligation to apply a safety standard be imposed by a medical facility by law.

There are basically two options. Either the obligation will be introduced in the ACS or in another, "sectoral" law. In the opinion of the authors, enshrining a similar obligation in the ACS is inappropriate, as it would disrupt its construction and purpose. The ACS affects only selected entities in various industries and defines a set of obligations for them. If specific sectoral regulations, in addition to obliged subjects other than those defined by law, begin to be added to the ACS, this appears to be unsystematic. For example, the Energy or Atomic Act also stipulates certain obligations in the field of information security, and in some cases its addressees are also the ACS addressees.

Thus, practice shows that the ACS and other, sectoral regulations, can coexist and complement each other. It therefore seems to be a suitable model to impose the obligation to comply with the security standard in a specific sectoral law, namely in Section 16 of Act No. 372/2011 Coll., On health services and the conditions for their provision (the Health Services Act), where the conditions for granting authorization to provide health services.

This would ensure the definition of clear measures to increase cyber security and the obligation to meet them as a condition for the provision of health services.

b) Who should meet the standard?

A seemingly simple question that is not easy to answer. To solve it, it is necessary to proceed from Act No. 372/2011 Coll., On health services and the conditions for their provision (the Health Services Act). As described above, regulation by the ACS is aimed at healthcare providers with inpatient capacity, and inclusion in the scope of the ACS is conditional on meeting special criteria of the type of entity and meeting impact criteria that filter out less important organizations that would find it very difficult to introduce mandatory regulation. The impact of the law is thus limited and a certain limitation of the scope of the addressees of the minimum-security standard, if it were mandatory, would also be necessary, because there are about 39,170 health care providers in the Czech Republic, and they are diametrically opposed entities. Due to this, it is appropriate to focus the standard on hospitals with inpatient care in a similar model as the ACS regulation is now set, but with lower limits.

c) Who will require and control compliance with the standard?

If we come to the conclusion mentioned in the previous part of the text, ie that the minimum security standard and the obligation to meet it would be a condition for the provision of health services, it would be appropriate that enforcement and control be entrusted to either the Ministry of Health as the central administrative office or, as in Section 15 of the Health Services Act,

> *"the regional authority in whose administrative district the medical facility in which the medical services will be provided is, the Ministry of Defense or the Ministry of Justice, if the health services are provided in medical facilities established by these ministries, or the Ministry of the Interior, in the case of health services provided in health care facilities established by this Ministry or in health care facilities established by the Office for Foreign Relations and Information or the Security Information Service."*

- **Setting standards for data sharing, establishing, and operating cyber security teams in healthcare sector**

A fundamental prerequisite for assuring cyber security in healthcare is establishment of a proper communication channel for efficient and fast data sharing in between individual health care providers and the government. The Ministry of Health as the top authority for the sector should provide such a channel. Paradoxically we are in a situation that the ministry disclaims from its coordinator role claiming that the cyber security area falls under another gestion based either on the NIS directive or specific law of a member state. In the Czech Republic, neither NCISA provides any specific communication channel that could be used by the OES operators in healthcare use to share cyber threat and attack information they are facing.

From the data sharing perspective, the subjects under the ACS are obliged to share information with the Governmental CERT team, which may based on the information issue a warning. Nonetheless, the Governmental CERT team is not specifically focused on healthcare and provides its services to all subjects under the CI or OES. It is also necessary to state that the Czech Ministry of Health has not established its own security team or a Security operations centre that could provide targeted support to healthcare providers.

As an appropriate collective intelligence solution, authors propose to create a hospital Security operation centre within a Ministry of Health. Such centre would not only act as a CSIRT/CERT team, which is often part of such a centre, but could also serve as a coordinator at both the national level and multinational level when collaborating through ENISA. Such centre would also be able to receive, test, and forward recommendations from other organizations and states[55] and should take part on forming new sector standards and recommendations.

This section analyzed the legislative measures following the attacks on hospitals in the Czech Republic in the period 12/2019 and 1/2021. The measures were evaluated and amendments to several decrees were proposed that could increase the cyber security of the healthcare sector. It was also proposed to create a sectoral platform for the exchange of security information and collective intelligence. Finally, it was proposed to introduce a minimum mandatory security standard for healthcare, which would prioritize safety from the point of view of hospital management.

8. CONCLUSION

The first part of the article analyzes the cyber incidents that took place in the period from 12/2019 to 1/2021 in health care facilities in the Czech Republic. All these incidents were caused by a combination of phishing and ransomware attacks. The use of ransomware along with phishing

[55] See also: *Procurement Guidelines for Cybersecurity in Hospitals*. [online] Available from: https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services/at_download/fullReport [Accessed 19 February 2021]. *Cloud Security for Healthcare Services*. [online] Available from: https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services/at_download/fullReport [Accessed 19 February 2021].

as an attack vector is common and not a new phenomenon, however, as it turns out, it is still effective. The attack on the Brno University Hospital can be assessed as the most fundamental of the analyzed incidents in terms of impact. These attacks sparked debate on the cyber security and resilience of hospitals.

NCISA also paid attention to the attacks on the healthcare sector. In response to incidents, they issued, inter alia, reactive measures and warnings in accordance with the Cyber Security Act. Through these actions, NCISA sought to respond to the security situation and oblige the addressees of these measures, primarily hospitals, to ensure security and vigilance. The issued measures were aimed at introducing measures against ransomware and phishing. The article analyzes these actions, especially the mentioned reactive measures, and proposes its own recommendations in connection with them.

As it turned out, the regulation of cyber security of hospitals, resp. health care in general is not sufficient and in 2020 only 16 hospitals out of the total number of 232 hospitals in the Czech Republic were within the scope of the Cyber Security Act. In 2021, NCISA amended the criteria for classifying organizations in the healthcare sector under the act with the aim of expanding its addressees. This change is then analyzed in the article. In the opinion of the authors, another legislative change would be appropriate, namely an amendment to Government Decree No. 432/2010 Coll., which would allow hospitals to be included in critical infrastructure, as no hospital meets the current criteria, and this situation seems inappropriate.

We are convicted that the findings described by us, as well as the criteria used to determine whether a health care provider will be considered an operator of essential services can be used in countries other than the Czech Republic.

The article further discusses the issue of introducing a minimum mandatory security standard in healthcare, which does not currently exist and which would cover healthcare facilities outside the scope of the Cyber Security Act. The authors recommend the creation of such a standard so that even organizations that do not fall within the scope of the Cyber Security Act have a clear framework on how to secure their systems.

A revised standard could also be issued for some specific threats. Due to the fact that the presented article analyzes attacks that combine a phishing campaign and ransomware, we will present a possible minimum standard related to these attacks.

LIST OF REFERENCES

[1] Cybersecurity & Infrastructure Security Agency (2020) *Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector* [online] Available from: https://us-cert.cisa.gov/ncas/alerts/aa20-302a. [Accessed 19 February 2020].

[2] Černý, V. (2020) *Dostupnost intenzivní péče pro hospitalizované pacienty s COVID-19.* [online] Available from: https://www.uzis.cz/res/file/covid/20200324-cerny-cz.pdf. [Accessed 19 February 2020].

[3] Davis, J. (2020) *Ransomware Causes 15 Days of EHR Downtime, as Payments Avg $111K.* [online] Available from: https://healthitsecurity.com/news/ransomware-causes-15-days-of-ehr-downtime-as-payments-avg-111k. [Accessed 19 February 2020].

[4] Davis, J. (2016) *Ransomware: See the 14 hospitals attacked so far in 2016*. [online] Available from: https://www.healthcareitnews.com/slideshow/ransomware-see-hospitals-hit-2016 [Accessed 10 May 2017].

[5] Delpy, B. and Le Toux, V. (2020) *Mimikatz.* [online] Available from: https://github.com/gentilkiwi/mimi-katz/releases. [Accessed 19 February 2020].

[6] Deutsche Welle (2020) *German police probe 'negligent homicide' in hospital cyberattack*. [online] Available from: https://p.dw.com/p/3ieQl [Accessed 19 February 2020].

[7] Donovan, F. (2019) *How Network Segregation, Segmentation Can Stop Ransomware Attacks.* [online] https://hitinfrastructure.com/features/how-network-segregation-and-segmentation-can-stop-ransomware-attacks. [Accessed 19 February 2020].

[8] Elshinbary, A. (2020) *Deep Analysis of Ryuk Ransomware.* [online] Available from: https://n1ght-w0lf.github.io/malware%20analysis/ryuk-ransomware/. [Accessed 19 February 2020].

[9] European Union Agency for Cybersecurity (2020) *Procurement Guidelines for Cybersecurity in Hospitals.* [online] Available from: https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services. [Accessed 19 February 2020].

[10] European Union Agency for Cybersecurity (2020) *Cloud Security for Healthcare Services.* [online] Available from: https://www.enisa.europa.eu/publications/cloud-security-for-healthcare-services/at_download/fullReport [Accessed 19 February 2021].

[11] European Union Agency for Cybersecurity (2020) *Procurement Guidelines for Cybersecurity in Hospitals.* [online] Available from: https://www.enisa.europa.eu/publications/good-

practices-for-the-security-of-healthcare-services/at_download/fullReport [Accessed 19 February 2021].

[12] Harašta, J. (2018) Legally critical: Defining critical infrastructure in an interconnected world. *International Journal of Critical Infrastructure Protectio*n, vol. 21, pp. 47-56. Elsevier. ISSN 1874-5482.

[13] Kolouch, J., Zahradnický T. and Kučínský A. (2021) *Cyber Attacks on Czech Hospitals in the Covid-19 Pandemic.* Unpublished manuscript.

[14] Landi, H. (2019) *Report: 40% of healthcare organizations hit by WannaCry in past 6 months.* [online] Available from: https://www.fiercehealthcare.com/tech/lingering-impacts-from-wannacry-40-healthcare-organizations-suf-fered-from-attack-past-6-months. [Accessed 19 February 2020].

[15] Mundo, A. (2019) *Buran Ransomware; the Evolution of VegaLocker.* [online] Available from: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/buran-ransomware-the-evolution-of-vegalocker/. [Accessed 19 February 2020].

[16] Proofpoint, Inc. (2020) *New Defray Ransomware Targets Education and Healthcare Verticals.* [online] Available from: https://www.proofpoint.com/us/blog/threat-insight/new-defray-ransomware-targets-education-and-health-care-verticals. [Accessed 19 February 2020].

[17] Sette, N. (2020) *Malware Analysis – Buran Ransomware-as-a-Service.* [online] Available from: https://www.kroll.com/en/insights/publications/cyber/malware-analysis-buran-ransomware-as-a-service. [Accessed 19 February 2020].

[18] The National Cyber and Information Security Agency (2020) *Cyberattack threat at the hospitals and other significant targets in the Czech Republic.* https://www.nukib.cz/cs/infoservis/aktuality/1425-hrozba-kybernetic-kych-utoku-na-nemocnice-a-jine-vyznamne-cile-cr/. [Accessed 19 February 2020].

[19] The National Cyber and Information Security Agency (2020) *NCISA issued a reactive measure for select health care subjects.* [online] Available from: https://www.nukib.cz/cs/infoservis/aktuality/1418-nukib-vydal-reaktivni-opatreni-pro-vybrane-subjekty-ve-zdravotnictvi/. [Accessed 19 February 2020].

[20] The National Cyber and Information Security Agency (2020) *Ransomware: Recommendations for Mitigation, Prevention, and Reaction.* [online] Available from: https://www.nukib.cz/download/publikace/pod-purne_materialy/Ransomware%20-%20Doporuceni_pro_mitigaci_prevenci_a_reakci.pdf. [Accessed 19 February 2020].

[21] The National Cyber and Information Security Agency (2020) *Recommended security measures to warning from 16th April 2020. Supplementary materia*l. [online] Available from:

https://www.nukib.cz/down-load/uredni_deska/Doporuceni_k_varovani_2020-04-17.pdf. [Accessed 19 February 2020].

[22] The National Cyber and Information Security Agency (2020) *Supplementary materials.* [online] Available from: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/. [Accessed 19 February 2020].

[23] The BBC (2016) *Three US hospitals hit by ransomware.* [online] Available from: https://www.bbc.com/news/technology-35880610 [Accessed 10 May 2017].

[24] Tracey, R. and Schmitt, D. (2020) *When Threat Actors Fly Under the Radar: Vatet, PyXie and Defray777.* [online] Available from: https://unit42.paloaltonetworks.com/vatet-pyxie-defray777/. [Accessed 19 February 2020].

[25] Trend Micro Incorporated (2017) *Defray Ransomware Sets Sights on Healthcare and Other Industries.* [online] Available from: https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/defray-ransomware-sets-sights-on-healthcare-and-other-industries. [Accessed 19 February 2020].

[26] Wadhwani, S. (2020) *Cyber World's Most Fearsome Ransomware Is Ryuk: SonicWall*. [online] Available from: https://www.toolbox.com/security/threat-reports/news/cyber-worlds-most-fearsome-ransomware-is-ryuk-sonicwall/. [Accessed 19 February 2020].