Received: 17. 9. 2020 Accepted: 1. 4. 2021 Published on-line: 15. 6. 2021
Available from: www.obranaastrategie.cz doi: 10.3849/1802-7199.21.2021.01.027-052

KYBERNETICKÁ BEZPEČNOST VE ZDRAVOTNICTVÍ

Poučení z případu benešovské nemocnice napadené ransomwarem Ryuk

THE CYBERSECURITY OF HEALTHCARE

The Case of the Benešov Hospital Hit by Ryuk Ransomware, and Lessons Learned

Ondřej Filipec[a], *David Plášil*[b]

Abstrakt

Tento článek se převážně zabývá kybernetickou bezpečnostní v oblasti zdravotnictví; specificky se věnuje případu benešovské nemocnice Rudolfa a Stefanie, která byla napadena ransomwarem Ryuk. Tento článek nejprve obecně rozebírá problematiku kybernetické bezpečnosti ve zdravotnictví a následně vyhodnocuje útok na nemocnici v Benešově. Pozornost je věnována zejména organizačním faktorům v procesu zvládání bezprostředních následků viru z hlediska kybernetické bezpečnosti a mikromanagementu. Hlavním cílem je zprostředkovat zkušenost se zvládáním kybernetického útoku a předat dobrou praxi pro ostatní aktéry. V souvislosti se šířením koronaviru a pandemie onemocnění COVID-19 kybernetická bezpečnost nemocnic dostává nový rozměr v rámci kritické infrastruktury státu.

Abstract

This article is dealing mainly with cybersecurity of healthcare with a special emphasis on the Benešov hospital (Czech Republic), which was hit by the Ryuk ransomware virus. The case shows that even a well-managed middle-size hospital with a relatively good level of cybersecurity might be significantly hit by the attack. The article first explores the general context of cybersecurity of healthcare with reference to the forms of cyber-attacks involving ransomware and then explores the case of the Benešov hospital (Hospital of Rudolf and Stefanie). The main aim of this article is to derive lessons learned from the case, which might be well used for the management of further incidents of similar nature, which is increasingly important at the times of fight with COVID-19 infection creating new pressure on the system.

[a] Department of Politics and Social Sciences, Faculty of Law, Palacký University in Olomouc, Olomouc, Czech Republic. Email: ondrej.filipec@upol.cz. ORCID ID: 0000-0002-9046-1577.
[b] Head of Information Technologies and Healthcare Technics Department, Rudolf and Stefanie Hospital in Benešov. Email: david.plasil@hospital-bn.cz.

Acknowledgement

This article has been written under the grant scheme of Jean Monnet Network Project 611293-EPP-1-2019-1-CZ-EPPJMO-NETWORK „European Union and the Challenges of Modern Society (legal issues of digitalization, robotization, cyber security and prevention of hybrid threats)“ awarded in 2019 to the Faculty of Law, Palacký University in Olomouc.

Klíčová slova

Kybernetická bezpečnost; zdravotnictví; nemocnice; ramsomware.

Key Words

Cybersecurity; Healthcare; Hospitals; Ransomware.

INTRODUCTION

This article is dedicated to the ransomware attack on a Czech hospital. On 11th December 2019, the hospital in Benešov (Hospital of Rudolf and Stefanie) was hit by a malware mix of Emotet-Trickbot-Ryuk. The main aim of the article is to analyse the attack and put it into deeper context of cybersecurity of healthcare with deriving lessons learned from the crisis caused by the virus. The article focuses mainly on the organizational factors of the cyberattack, which are strengthened by security dimension. The focus on the organizational factors and the level of security is both practical and rational because there are some restrictions in the access to information. Due to security nature of the issue and investigation by the police, some information regarding the case is confidential and thus will be not disclosed (e.g., vector of the attack). Instead, next to the broader context and detailed information about the case, the article provides direct experience of the attack as one of the authors was directly involved in the incident response team. Authors are convinced that the Ryuk attack from 11th December 2019 may serve as a good example (ransom was not paid, no data were lost, key systems were restored within a week, and the security incident led to a great improvement in the IT security), which might be used by other IT or security specialists.

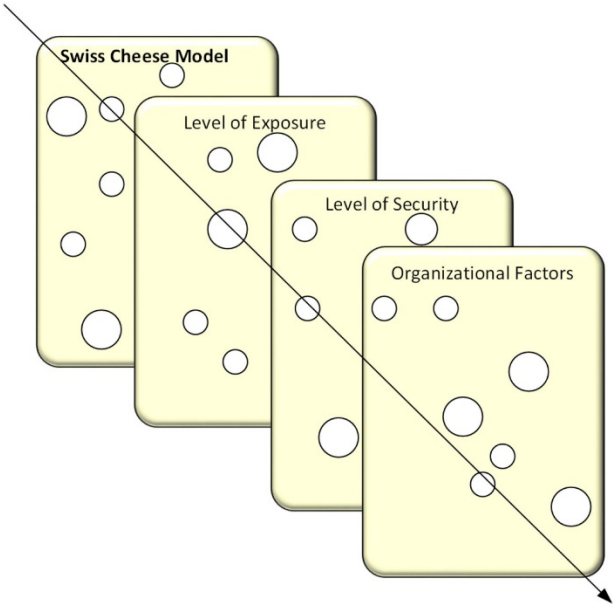
Next to the provision of unique professional experience, this article has also other added value. First, the quality of information in the public space varies, as some information was selectively communicated and processed by media. This article is based on a primary research. Second, the literature about the case is almost non-existent. Small exception is the article by Adam Kučínský and Vojtěch Sikora which was published in spring 2020.[2] Authors of this short article provided one of the first attempts to develop the issue in the academic context. Hopefully, this article will provide also some more general context and practical recommendations how to enhance security in hospitals, which is a crucial domain at the times of Covid-19. Without IT systems, hospitals cannot work effectively.

The principal research question leading to exploration of good practice and lessons learned is: What organizational and security factors contributed to good management in the post-attack period? Answer to this question may help other hospitals to manage large-scale cyber-attack. The main analytical framework in the article uses the "Swiss Cheese" concept presented and developed by Alexander McLeold and Diane Dolezel.[3] The concept was originally created by James Reason and developed by other authors including Faouzi Kamoun and Mathew Nicho or James Stein and Kurt Heiss.[4] In the "Swiss Cheese" concept, there are three slices (exposure, security level and organizational factors) whose holes present vulnerability. When the holes line up then the likelihood of a successful breach

[2] KUČÍNSKÝ, Adam – SIKORA, Vojtěch. Malware Emotet – Trickbot – Ryuk v benešovské nemocnici. *Data Security Management*. 2020, 24(1), 39–43.
[3] MCLEOLD, Alexander – DOLEZEL, Diane. Cyber-analytics: Modelling factors associated with healthcare data breaches. *Decision Support Systems*. 2018, 108, 57–68.
[4] REASON, James. The contribution of latent human failures to the breakdown of complex systems. *Philos. Trans. R. Soc. Lond. B Biol. Sci*. 1990, 327, 475–484; KAMOUN, Faouzi – NICHO, Mathew. Human and organizational factors of healthcare data breaches: the Swiss cheese model of data breach causation and prevention. *Int. J. Healthc. Inf. Syst. Inform*. 2014, 9, 42–60; STEIN, James E. – HEISS, Kurt E. The Swiss cheese model of adverse event occurrence—closing the holes. *Semin. Pediatr. Surg*. 2015, 24, 278–282.

occurs.[5] It is important to note, that it is possible to have more slices (security-relevant layers) as, for example, organizational factors may be divided into material or human resources related. The model is presented in Figure 1.

Figure 1: The Swiss Cheese Model



Source: MCLEOLD – DOLEZEL, 1990[6]

While the exposure level seems to be an externally driven factor connected with the encouragement and persistence of the attacker, the security level and organizational factors are merely internally driven. As pointed out by McLeold and Dolezel, holes are not stable in time. They change size or even position. Some might get closed and some might get bigger over time. If we take into account the perspective of variability, individual slices are also not equal and they might get bigger or smaller, depending on the number of measures involved. As pointed out by McLeold and Dolezel, there are several studies dealing with important internal factors.[7] Based on various studies[8] they identify six areas:

[5] REASON, ref. 3, pp. 475–484.
[6] MCLEOLD, Alexander – DOLEZEL, Diane. Cyber-analytics: Modelling factors associated with healthcare data breaches. *Decision Support Systems*. 2018, 108, 61, based on: REASON, James. The contribution of latent human failures to the breakdown of complex systems. *Philos. Trans. R. Soc. Lond. B Biol. Sci*. 1990, 327, 475-484.
[7] Ibid.
[8] DA VEIGA, Adéle – ELOFF, Jan H. P. A framework and assessment instrument for information security culture, *Comput. Secur*. 2010, 29, 196–207; Ponemon Insitute. Cost of data breach: United States, Ponemon Research Report, Ponemon Institute, 2010; KOBUS, Theodore J. The A to Z of healthcare data breaches. *J. Healthc. Risk Manag*, 2012, 32, 24–28; WIRTH, Axel. The importance of cybersecurity training for HTM professionals, *Biomedical Instrumentation & Technology*. 2016, 50(5): 381-383; KHALFAN, Abdulwahed Mohammed. Information security

1) employee behaviour aligned with security culture; 2) adoption of best IT governance practices; 3) effective policies and procedures for handling personal health information; 4) ongoing security training for employees; 5) attention to selection of vendors and their handling of personal health information; and 6) implementing a strong risk management procedure.[9] These factors will also be, when possible, explored in the case of the Benešov hospital.

However, the above model may be approached also in the critical way as it is hard to exactly define individual slices. In the visual representation of the model, all slices appear separately, however, in reality, organizational factors are very connected to the level of security. In fact, both slices are influencing each other as organizational factors might change the level of security and vice versa. For that reason, in the following analysis both factors are revealed with a special focus on the data security (security of network, servers, end stations, data loss prevention) and organizational factors with special reference to activities leading to the crisis IT management. In this sense, organizational factors are understood in a restricted way - aimed at IT security, not the management of the institution in general. It is important to note that it is not an individual slice which makes a target vulnerable, but a set of systemic variables and a sequence of activities which lead to vulnerability. Factors are interacting. Alexander McLeold and Diane Dolezel are going further and discover relations between individual slices. For example, in their study they discovered that increased connectivity (e.g., point of access to the IT system) increases the opportunity of a security breach as more employees are involved in the process. The larger the organization (departments using IT systems), the higher odds of a security breach,[10] and the same applies to the other important organizational factors, such as age: the older the organizations are, the more prone they are to security breaches. This may be due to the newer technologies involved, less legacy systems or simply a better IT infrastructure. Also, technology can increase the level of security through a number of measures including biometrics, barcoding or radio frequency identification.[11] In other words, vulnerability of healthcare institutions is composed of multiple technical and organizational factors or at a certain level of abstraction: variables. Every attack is unique due to its different scope, length, tools involved or aim and the present unique set composing an independent variable. The consequences of the attack may be considered as a dependent variable, however influenced by the level of security and organizational factors presenting numerous intervening variables.

In the risk assessment, there is a simple formula: Risk (R) = Likelihood (L) x Damage (D). Damage may be calculated as the number of victims affected by the attack, material or non-material loss (e.g., damaged image, decreased trust, etc.). It is important to note that the likelihood and damage are negatively correlated: with the increasing (expected) damage of the attack, the likelihood of such an attack decreases. This is due to increased

considerations in IS/IT outsourcing projects: a descriptive case study of two sectors. *Int. J. Inf. Manag.* 2004, 24, 29–42.

[9] MCLEOLD – DOLEZEL, ref. 2, p. 61

[10] As of February 2020, in the vast majority of cases Ryuk was used to attack enterprises, not physical persons who are merely subject of sextortion e-mails. This information, however, cannot be interpreted that "small" is not interesting. Even small devices with little computer power might be part of gigantic botnets used for large scale cyberattacks.

[11] MCLEOLD – DOLEZEL, ref. 2, p. 66

material, operative or the human resources cost of the attack as big attacks usually require more skills, initial resources and time. However, this simple relationship may be distorted by the rapid progress of technology, increased availability of powerful hardware and software allowing faster decryption or other developments temporarily empowering attackers over victims. It is necessary to keep in mind that hackers are creative people who will try to be a few steps ahead. As a result, focus on preventive measures might devaluate compared to reactive measures taken based on ex-post experience. In the worst-case scenario, hackers might become superior and dominate: a state similar to the "Black Swan Effect" or "Wild Card", as described in the security literature, for the occurrence of an unthinkable and unexpected situation having a dramatic impact on society and presenting "revolution" in the development of the phenomenon. For example, as the 9/11 attack might be considered a Black Swan effect in the area of terrorism, similarly the hack of a national cloud or getting military grade artificial intelligence under the control of a hacker might be a similarly important event in cybersecurity. For this reason, it is necessary to treat every incident seriously as it might bear some features of a future monster attack.

The article is divided in three parts. The first part is the introduction to the topic and it provides necessary insight into the issue of ransomware and cybersecurity of healthcare. It also serves as the literature overview on the issue. The second part is dealing with the Benešov hospital case, which is explored in line with the "Swiss Cheese" framework. This part is dedicated to all three slices including the level of exposure, the level of security and the organizational factors. Due to reasons mentioned above (restriction on information), individual slices are imbalanced as the main focus is put on the organizational factors, mainly in relation to the successful management of the attack. This part is divided into sections – initially the security environment of the Benešov hospital is introduced, then the article provides details about the attack and first five days after and its last section deals with the mid-term response and recovery. The last – third part of the article – is dedicated to the lessons learned with recommendations provided based on a direct experience of one of the authors.

RANSOMWARE AS A THREAT TO CYBERSECURITY

Ransomware and crypto viruses are an increasingly important threat for hospitals worldwide.[12] Hospitals are vulnerable due to the rapid progress of information technologies collecting data from clients outside the hospital environment, which increases the possibility of security breaches or generally the increasing digitalization of healthcare on one side and valuable data storage on the other side. As estimated, a complete set of media credentials may be valued at 1000 USD on the black market:

[12] VAN ALSTIN, Chad Michael. Ransomware: It's as scary as it sounds. But with security best practices, you can fight back. *Health Manag Technol*. 2016, 37(4), 26–27; KRUSE, Scott Clemens – FREDERICK, Benjamin – JACOBSON, Taylor – MONTICONE, Kyle D. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care,* 2017, 25, 1–10.; FARRINGER, Deborah R. Send Us the Bitcoin or Patients Will Die: Addressing the Risks of Ransomware Attacks on Hospitals. Seattle University Law Review. 2017, 40(3), 937–986; COVENTRY, Lynne – BRANLEY, Dawn. Cybersecurity in Healthcare: A narrative review of trends, threads and ways forward. *Mauritas* 2018, 113, 48–52.

a stolen medical identity might be used, for example, for medical prescriptions or getting access to health services.[13] Data of clients are an important commodity for hackers and ransomware uses the same logic.

A special study of the Ponemon Institute shows that 69% of hacker attacks are profit oriented. However, the average income from an attack is relatively low at 28.744 USD per year for an average of 705 hours of attacking.[14] However, this trend may change due to the increasing availability of automated attacking software, increasing computing power or advanced forms of cooperation and organization among hackers. Due to various reasons, there will be always enterprises with a low level of security, which are vulnerable to the attack that might exploit the vulnerability. The threat is asymmetric. A billion-dollar hospital might be out of order for weeks after a successful attack. The primary cost is twofold: first, health and sometimes the life of citizens is endangered, and second, there are financial costs associated with the attack regardless of the payment of ransom: restoration of IT systems and their protection is costly and also the income of the hospital is limited due to interrupted and limited services. The ransom for data decryption in the case of Ryuk varied from tens of thousands USD to a million USD per incident.[15] During the Covid-19 pandemics, hospitals are often on an edge of possibilities and simply cannot run out of order without a direct impact on health services provided. In this respect, hospitals are under constant pressure during the pandemic and so are their IT departments that have prevent penetration of the systems by malware. This urgency has also been exploited by hackers. For example, as reported by NUKIB, the number of cyberattacks during the pandemics has increased and they have become more targeted.[16]

According to a large study conducted on 1,176 targets victimized by the ransomware, in total, 61.3% of victims did not paid the ransom. Out of this number, 53.3% succeeded in recovering the data. On the other side, 38.7% of victims paid the ransom. Out of this share, 19.1% recovered the data and the remaining 19.6% lost the data.[17] In other words, the payment of ransom led to data recovery in about half of the cases, if we take into account the logic that those who recovered the data refused to pay the ransom. It is necessary to mention, that there are some principal issues related to the payment of ransom. First, the payment of ransom is encouraging further attacks as it proves to the attacker that the ransomware business model works. As a result, other attackers might be encouraged to start. Second, payment of the ransom involves some sort of stigmatization: paying institutions are not proud to present that they have paid, which might limit their willingness to cooperate with relevant authorities or even lead to the

[13] Ibid, p. 49.
[14] PONEMON INSTITUTE. Flippin the Economics of Attacks [online]. Ponemon Institute, January 2016 [cit. 2020-07-29]. Available from: shorturl.at/bemrK.
[15] COHEN, Jessica Kim. Washington hospital refuses to pay $1 million ransomware demand [online]. *Modern Healthcare*, 15. 8. 2019 [cit. 2020-07-29]. Available from: shorturl.at/ipI36.
[16] NUKIB. *Vyděračské útoky ramsomwarem jsou cílenější: míří na velké firmy, státní a veřejné instituce*. NUKIB, 7. 8. 2020. [cit. 2020-12-15]. Available from: shorturl.at/c1579.
[17] CYBER-EDGE. Cyberthreat Defense Report [online]. Cyberedge Group, 2018 [cit. 2020-07-29]. Available from: shorturl.at/xzCOP.

decision not to report the incident to the authorities.[18] Third, even when ransom is paid and data recovered, there is the necessity of investment to improve security and change defensive measures because the cyberattack revealed a vulnerability which might soon be exploited by other attackers. In this sense, the unified approach of the institutions involving a "no undercut policy" may help to keep a line against attackers and prevent or minimalize attacks on hospitals. When hackers know that hospitals are not paying, there will be less incentive for an attack as the majority of cyberattacks are profit oriented.

Data recovery is a sensitive issue and requires expert advice. In the case of the Benešov hospital, the process of recovery was coordinated with the national authority (National Cyber and Information Security Agency - NUKIB), which verified data consistency and security measures. As pointed out by Kučínský and Sikora, it is often the mistake of administrators who decide on data renovation when the system has not been cleaned from the previous infection.[19] As a result, in the worst-case scenario the encryption process may start again having much more serious consequences.

However, hospitals may also face smaller security breaches which might influence the usability of some devices or disrupt data integrity.[20] Some of the malfunctioning medical devices may have an impact on the health of patients.[21] Hospitals operate various devices necessary for keeping people alive. From cardio stimulators to infusions and intubations, monitoring devices in the intensive care units etc. Despite the fact that most of the devices are connected to separate networks, experts can imagine switching off or disruptions that are life threatening. Also, more basic activities such as medication schedules including the type of medicine and quantity or operation schedules are sensitive to mistakes and may cause problems.

To research how many deaths or injuries are caused by cyber security breaches is problematic due to the multi-causality of the phenomenon. Some devices might not work properly without being noticed and accidents may occur as a result of a human mistake. There is simply a lack of direct evidence.[22] For this reason, the available data are based on estimations. For example, as noted by Harold Thimbleby and Martyn Thomas (2018), just in the UK it is estimated that more than 900 people per year die because of poor NHS computer systems. They claim that the Wannacry cyberattack crippled 37 trusts and resulted in the cancellation of 20,000 appointments in 2017, which could have killed some patients.[23]

[18] In some countries, reporting incidents is not mandatory or provisions of the act are not clear enough to specify, for example, what a "significant" attack or what "reporting in reasonable time" mean.
[19] KUČÍNSKÝ – SIKORA, ref. 1, p. 41.
[20] CORONADO, Anthony J. – WON, Timothy L. Healthcare Cybersecurity Risk Management: Keys To an Effective Plan. *Biomedical Instrumentation & Technology: Cybersecurity In Healthcare*, 2014, 48(1), 26–30; WU, Fubin – EAGLES, Sherman. Cybersecurity for medical device manufacturers: Ensuring safety and functionality. *Biomed Instrum Technol*. 2016, 50(1), 23–33.
[21] ANDERSON, Scott – WILLIAMS, Trish. Cybersecurity and medical devices: Are the ISO/IEC 80001-2-2 technical controls up to the challenge? *Computer Standards & Interfaces*, 2018, 56, 134–143.
[22] FU, Kevin – BLUM, James. Controlling for cybersecurity risks of medical device software. *Commun ACM*. 2013, 56(10), 35–37.
[23] THIMBLEBY – THOMAS cited in GONNELLY 2018.

Their estimations are supported by a study measuring the negative effects of cyberattacks on heart attack responses. Hospitals affected by a cyberattack have a higher average response time to heart attacks, resulting in additional 36 deaths per 10,000 heart attacks per year. In other words, hospital time-to-electrocardiogram increased by as much as 2.7 minutes and 30-day acute myocardial infarction mortality increased by as much as 0.36 percent during the three-year window following the breach.[24] However, it is necessary to note, that these correlations might be affected by intervening variable or stay on false correlation (for example, slower reaction of the hospitals might be caused by underfinancing, which might explain also the lower level of IT security and more frequent breaches). However, a successful attack may lead to life losses, which raises the issue of cyber terrorism. Hackers may use the "denial of care" in the future for political purposes or ransom payments not far from acts of "criminal terrorism" where political motivation is not usually a crucial aspect of the act.

The malware dealt with in this article is called Ryuk. Ryuk is a typical type of ransomware which is being activated after a sequence of attacks removing security barriers in order to encrypt data and demand ransom from enterprises. As pointed out by Subash Poudyal, Kishor Datta Gupta and Sajib Sen (2019), Ryuk succeeded in getting 640,000 USD in ransom payments in a single wave in the US.[25] However, experts from the CrowdStrike internet security company claim that just between August 2018 and January 2019 Ryuk was responsible for 52 ransom transactions, which netted over 705.8 bitcoins, equal to 3.7 million USD. The value of ransom varies according to the size of the organization: the lowest observed ransom was 1.7 bitcoins and the highest 99 bitcoins.[26]

Ryuk has developed from previous ransomware called Hermes, which was distributed in February 2017 and available on various forums for just 300 USD with the other necessary e-equipment including two built-in e-mail addresses, decryptor (a code allowing to decrypt the text) and a unique RSA key[27]. Later in mid-August 2018, a modified version of Hermes appeared as Ryuk, which is associated with the Russian eCrime group WIZARD SPIDER operating TrickBot banking spyware. However, the origins of Hermes, from which Ryuk has developed, may be tracked to the North Korean STARDUST CHOLLIMA group – publicly reported as the "Lazarus Group".[28] STARDUST CHOLLIMA is focusing on abusing the Society of World Internal Financial Telecommunications (SWIFT) systems and international banking transactions.[29] It is not surprising that suspected actors are coming from two countries suffering financial isolation due to sanctions and the absence of or

[24] CHOI, Sung J. – JOHANSON, Eric M. – LEHMANN, Christoph U. Data breach remediation efforts and their implications for hospital quality. *Health Serv Res*. 2019, 54, p. 975.
[25] POUDYAL, Subash – GUPTA, Datta Kishor – SEN, Sajib. PEFile Analysis: A Static Approach To Ransomware Analysis. *The International Journal of Forensic Computer Science*, 2019, 14(1), p. 35.
[26] CROWDSTRIKE. Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware [online]. CrowedStrike, 10. 1. 2019 [cit. 2020-07-29]. Available from: shorturl.at/pxBO9.
[27] RSA Key refers to a private key based on RSA algorithm (developed by Ronald L. Rivest, Adi Shamir and Leonard Adleman). RSA is asymmetric encryption algorithm with two keys – one to encrypt and other to decrypt. It is a tool for digital signatures and authentication.
[28] Ibid.
[29] CROWDSTRIKE. Meet CrowdStrike's Adversary of the Month for April: STARDUST CHOLLIMA [online]. CrowedStrike, 6. 4. 2018 [cit. 2020-07-29]. Available from: shorturl.at/nqyW2.

non-functional rule of law. Both countries might be hacker-friendly as hackers often work in line with state interests.[30]

According to Kučínský and Sikora, the increased activity of Emoted was evidenced at the end of October 2019 when the analysis aimed at logs from honeypots and the sinkhole servers of foreign partners showed a much higher activity than usual together with the first news about the renewed activities of revealed and switched-off C&C servers.[31] The malware "trinity" Emotet, Trickbot and Ryuk soon hit the hospital in Benešov. The attack on the hospital was extensive and synchronized with other attacks in the Czech Republic. As a result, the OKD mining company was also hit with the same combination of malware and ransomware.[32] Similar to the Benešov hospital, OKD was also paralyzed due to the attack and mining activities were stopped. OKD resolved the attack much more quickly as a parallel network was quickly created, while the main life support systems (e.g., methane sensors) were not connected to the main network.[33] However, despite the fact that this the company did not publicly announce the cost of the damage, the expected costs might well be in the millions of Czech korunas.

THE BENEŠOV HOSPITAL CASE

This part deals with the security incident in the Benešov hospital. For the purposes of a complex analysis there are three sections. The first section provides an overview of the IT security environment of the Benešov hospital and brings attention to some of the key elements of the system prior the attack. The second section maps the first five days after the attack with a detailed description of conducted activities while attempting to draw implications. The third section is dedicated to the mid-term response. In the context of the "Swiss Cheese" framework, the following parts focus merely on organizational factors with orientation on the IT infrastructure. The approach used in all three sections is chronological, which allows us to follow the story of Ryuk with its implications developing over time.

Security Environment of the Benešov Hospital

It is important to note that cybersecurity in hospitals in the Czech Republic was considered a secondary issue for a very long time. The state was supported by the fact that hospitals had not been previously covered by the Cybersecurity Act and as a result only limited attention was given to their cybersecurity. This is a paradox as Czech

[30] For example, in June 2017 Vladimir Putin said: "*Hackers are free people, just like artists who wake up in the morning in a good mood and start painting. Likewise, hackers get up in the morning and read the news about international affairs. If they feel patriotic, they try to make what they see as fair contribution to the struggle against those who speak ill of Russia*" RADIO FREE EUROPE. Putin Compares Hackers TO "Artists", Says They Could Target Russia's Critics For "Patriotic" Reasons [online]. Radio Free Europe, 1. 6. 2017 [cit. 2020-07-29]. Available from: shorturl.at/dmrS5. However, it has to be noted, that after this favourable statement Putin added, that Russia is trying to fight hackers in Russia.
[31] KUČÍNSKÝ – SIKORA, ref. 1, p. 39.
[32] Ibid.
[33] CT. *Benešovská nemocnice, kterou napadl hacker, je po téměř třech týdnech v plném provozu* [online]. Česká televize, 30. 12. 2019 [cit. 2020-07-29]. Available from: shorturl.at/jtzP3.

hospitals had had some experience with ransomware. Recently, for example, the Motol hospital in Prague, Brno Faculty Hospital or Faculty Hospital in Hradec Králové were under attack. In June 2018, the hospital in Janov was hit with ransomware demanding a payment in bitcoins. After the attack, employees in the hospital lost access to information systems.[34] According to the Kaspersky research from 2019, approx. 19% of Czech hospitals experienced some cyberattack.[35] From the previous development it might be estimated that most of the hospitals were not hit by ransomware, but by phishing attacks. It is estimated that 90% of attacks against hospitals are phishing or spear-phishing[36] attacks with an increasing sophistication.[37]

In its Report on the State of Cyber Security in the Czech Republic in 2018, the National Cyber and Information Security Agency noticed three important threats regarding hospitals: 1) lacking standards of cybersecurity in the hospitals, which remained out of regulatory standards vis-á-vis novelization that had covered only hospitals with the capacity of 800+ beds or hospitals specialized in traumatological care since 1 October 2017; 2) old software in a "considerably high number" of hospitals and 3) the risk of patient data misuse due to the relatively high accessibility to various persons including hospital employees, suppliers, etc., who might misuse unauthorized or authorized access to steal data and sell it on the black market.[38]

The Benešov hospital is a middle-size hospital with a natural and factual catchment area of 120,000 people. However, during summer this number might be twice as high as the hospital is located in a holiday-attractive region and the annual report of the hospital claims a catchment area of 400,000.[39] As in the case of other hospitals' networks, the network is a very complex system which is very distributed across many departments and pavilions. The network in Benešov had a very robust elements at the primary network but used also separated networks. In practice, it is a complex of eight buildings with some centres of excellence. The hospital received award for quality several times and is considered the best in the region. The hospital is composed of 22 main departments, including surgery, oncology, clinical microbiology or department of anaesthesiology and intensive care unit. Hospital had 411 beds and approx. 760 employees.[40] However, some connections might lead out of the hospital (Open VPN and Microsoft VPN).[41] It is also

[34] NUKIB. Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2018 [online]. Národní úřad kybernetické bezpečnosti, 2019 [cit. 2020-07-29]. Available from: shorturl.at/aioN0.
[35] CT24. Za útokem na benešovskou nemocnici byl ruský vir Ryuk [online]. Česká televize, 14. 1. 2020 [cit. 2020-07-29]. Available from: shorturl.at/FV025.
[36] Both phishing and spear-phishing attacks are aimed at tricking the target to share sensitive information (e.g., passwords). While phishing attacks are more general and random, spear phishing attacks are targeted at an individual. Attackers are first trying to get as much as possible background and personal information in order to create a more trustworthy e-mail. Spear-phishing attacks are more aggressive, theoretically more successful (in proportion to the number of addresses sent) but are also more time consuming.
[37] NUKIB, ref. 32.
[38] Ibid.
[39] BENEŠOV HOSPITAL. Výroční zpráva Nemocnice Rudolfa a Stefanie Benešov. Nemocnice Rudolfa a Stefanie Benešov, 2020a [online] [cit. 2020-07-29]. Available from: shorturl.at/ajkwF.
[40] Ibid.
[41] VPN refers to the Virtual Private Network, allowing to connect a computer to a network via encrypted connection.

necessary to mention that the IT infrastructure developed over time. As a result, expansion of IT was gradual and, in many cases, underfinanced. The situation is different from newly established enterprises with their IT infrastructure on a "green field". In other words, when a hospital starts from the beginning, updating and renovation of the workstation requires interruption in the service. And this might be a problem for some managers or doctors as they need to use the work station and interruptions in work are undesirable.

The number of beds (especially acute beds) is a necessary indicator for being covered under Czech cyber-security law. Because of the number of beds below the threshold, the Benešov hospital does not fall under the cyber-security act, both with positive and negative effects. It is beneficial that the hospital has more freedom to decide about the IT, it is not so much under control and not forced to invest a lot of money into the IT, but on the other hand, this has direct impact on IT security, not being forced to follow standards set by NUKIB. Before the attack, the hospital actively implemented management of the network, data loss prevention (DLP) and segmentation.

The server environment was characterized by a great proportion of servers running in the old virtual environment, there were various versions of MS Windows and Linux. Before the attack, there was an ongoing installation of new VMware, including new HW (servers and disk arrays). End stations were equipped with Windows 10 or Windows 7, devices with Windows 7, Windows 10, Embedded, and 2 devices without connection to the network had Windows XP. The ongoing works were dedicated to securing the end station by DLP. From the IT perspective, the Benešov hospital had approx. 300 computers and workstations.[42] However, in fact, the number might have been twice higher when counting also laptops and other devices.

Regarding investments and IT infrastructure, the Benešov hospital was on average in comparison to other hospitals in the Czech Republic. Before the incident, there were many hospitals in the Czech Republic with approximately similar level of IT security. The situation in the Czech Republic is slightly different in faculty hospitals, which have different access to money and different teams, and regional hospitals at a similar level. For IT security in hospitals, the attitude of the management is important: when there is a manager who understands IT, then it is more likely that IT will receive more money. Moreover, this situation is characteristic for almost every hospital.

The hospital in Benešov is an accredited hospital, which had a system of IT training for employees in place. The system, procedures and trainings were working for some years. However, the fact that people sit somewhere and listen to information about new trends in the cyber security may not prevent "clicking" on an e-mail or document, which might be a pretext for a cyber-attack. Despite the fact that the hospital had all documents, security strategies, scenarios and set up procedures, they did not play a significant role when the incident occurred. During an attack, reactions are spontaneous and people act in accordance with simple logic and common sense. Reaction is merely *ad hoc*. This might be because documents may not be up-to-date and real needs of the hospital may change in time. It means that during the crisis some systems have greater priority than another. To have some "grand rulebook" with all possible situations may be not effective as

[42] BENEŠOV HOSPITAL. *Historie a současnost* [online]. Nemocnice Rudolfa a Stefanie Benešov, 2020b [cit. 2020-07-29]. Available from: shorturl.at/oxKU5.

a single paper with 10 points from the "to-do list" and 10 systems which shall be running. The Benešov experience suggests that the first most important thing is to physically disconnect back-ups from the system and take care that back-ups are safe. This implies that the key activity of the data management is data back-up. In the case of the Benešov hospital, the system made back-ups several times per day in some cases. Almost every day full back-ups were made with a minimum once per week. Some data were directly transferred to the strongbox. Because libraries are usually slow, the Benešov hospital had two independent storage fields for both online and offline back-ups.

The hospital used anti-viruses and a firewall, however, this is only one element in the whole system and in general anti-viruses do not provide complete security. The hospital used an old firewall which had a limited power for complex solution of the system. Similarly important issue is updating the workstations. This might be not due to omission but just because they are not used so often or just because more urgent issues are attended to. Therefore, it is necessary to have a complex solution and antivirus is just a part of it. Very important role shall be attributed to the protection of end-stations, which is a very demanding and long-term task. In Benešov, the internal security was based on several instruments. For example, there were two passive probes within the network – one of the probes for the hospital. This one was used for proper monitoring of the network to observe what is going on. The second passive probe was installed within a project of the Central Bohemian Region – this probe is now collecting data about activities and every month these data will be evaluated. The second tool is monitoring of individual activities, which allows to observe what individual users are doing at the end stations. Unfortunately, the IT department of the hospital does not have personal capacity to fully verify all logs and perform search.

The First Five Days

In the first phase, e-mails of the hospital were subject to a massive spam and phishing campaign. The catalyst seems to be probably a fake invoice sent in one of the e-mails which looked very trustworthy. A click on the invoice initiated the virus called "Emotet".[43] (Chvojka, cited in Shabu 2020). However, as pointed out by Kučínský and Sikora (2020: 40), up till now the mechanism of penetration was not fully investigated. For this reason, the authors mention the increased sophistication of phishing campaigns: early campaigns were triggered with users recognizing very bad language of the messages and mistakes in grammar. However, contemporary phishing campaigns have very advanced language and sometimes they also use previous communications from the compromised e-mail boxes in order to increase trust.[44] In the case of Benešov, Emotet succeeded in overcoming the firewall and two updated antivirus systems.[45] This malware soon mapped all processes in all of approx. 300 CTS systems (including the back-up server) of the hospital and via cloud it reported back to the attacker that the virus was in and the network was under control.[46] The virus continued the attack downloading the "Trickbot" virus from the cloud. Trickbot served as the Troyan horse and its task was to

[43] SHABU, Martin. *Ukliknutí „stálo" nemocnici v Benešově 40 milionů. Kyberútok začal otevřením přílohy* [online]. Lidovky.cz, 16. ledna 2020 [cit. 2020-07-29]. Available from: shorturl.at/fART2.
[44] KUČÍNSKÝ – SIKORA, ref. 1, p. 40.
[45] CT, ref. 33.
[46] SHABU, ref. 41.

map all passwords including privileged accounts from administrators with most powers over the system. As a consequence, Trickbot discovered where all the passwords were located and contributed to the escalation of privileges. It enabled spreading to other computers and encrypting data there. Kučínský and Sikora (2020) note that an average user is not able to recognize that the system is under attack. Most probably the first one to know is the server admin at the moment when Trickbot starts contacting suspected address and asking more instructions.[47] Having access to all passwords, the ground was ready for the Ryuk ransomware.

Everything started on Wednesday 11 December 2019 at 2:50 in the morning when the head IT specialist got phone-call that the STAPRO FE application did not work. Just after 2 am, the staff of the surgery ambulance realized that the system was very slow and that the application for doctor's documentation was not working properly. It looked like an update of software, however, in reality this was the final stage of a cyberattack (see, for example, ČTK 2019). The malware which penetrated the system most probably already before midnight was just finishing the encryption of data. Mr. Plášil was very soon back at work and at approx. 3:10 he analysed the issue. He discovered a non-standard update of the software. The application was controlling its binary data on a disk and verifying whether they were updated. When data are not up-to-date, then STAPRO FE is downloading update from a saturation server. In this case, it already started to download the encrypted version and malware was recognized from the suffixes of the infected files. At 3:13, STAPRO FE was contacted and soon, approx. at 3:30, there was serious suspicion about the crypto virus. As a result, the IT specialist physically disconnected GBIC modules[48] from the central switch. Despite this hard interference, many systems were paralyzed. However, it is necessary to note that even an earlier reaction would not have been effective, because encryption most probably started before midnight and around 2 am it was already finished. Nonetheless, the physical disconnection of the star arrangement interrupted encryption activities in the direction to end stations. It is also important to note that analysing the disk for discovering the exact date and time is a very long process and, in fact, this information was available almost one month after the disks were given to the analysis.

Between 4:00 and 5:00 in the morning, the IT team was already at the place, later joined by a team form the external company which analysed samples. Together, the server infrastructure was transferred into the minimal state which meant that the hospital "returned in time" by 30 years and changed from an e-hospital into a "paper hospital", significantly restricting the provided health services. Approx. between 5:00 and 8:30 an Emergency Task Force (ETF) was set up, which analysed the problem and started communication with partners. ETF provided all necessary information to the founder of the hospital (Central Bohemian Region), press, police, and law enforcement authorities. The issue was addressed also with our data protection officer and NUKIB. One of the initial steps was informing the emergency hotline 112 not to transport patients to the hospital. This communication was effective because patients were transferred to other hospitals, which were informed in advance. The positive element in this measure was a fact that the director had close connections to the emergency service and everything was communicated effectively. Patients were advised not to visit the hospital, which

[47] KUČÍNSKÝ – SIKORA, ref. 1, p. 40.
[48] It refers to a Gigabit interface convertor – a standard transceiver, which is hot swappable.

prevented delays and in some cases health deterioration due to non-operability of the hospital. Also, Czech Police (regional headquarters) initiated investigation and samples of encrypted data were transferred approx. at 8:30. It is necessary to note that there was no information about ransom found, just an e-mail contact. Later it was discovered that data were encrypted using a relatively strong RSA-4096 and AES-256 key, which is currently impossible to decrypt.

During Wednesday, 11 December 2019 first logs were sent to ESET, which later set up a mobile laboratory in the hospital to analyse the virus, collect data and provide recommendations. During the afternoon, cooperation with NUKIB fully started with the issue analysis, transfer of logs and back-up recovery from the SYNOLOGY disk. NUKIB sent its incident response team to the place, including a forensic specialist, to research the type of the attack and scope of the infiltration and to collect other background information about the attack, which might be later used in the criminal procedure. Analytics covered the analysis of Windows domains, Windows stations, forensic analysis of Windows and Linux, network system and monitoring and visualization of the infrastructure.[49] IT support from the Na Homolce hospital in Prague was provided. During the evening, the infrastructure was reconciled and the response team was waiting for the log analysis, considering the duplication of back-ups. This soon turned to be very a good decision. SYNOLOGY is composed of approx. 24 disks, but because of recording data all the time the devices are not physically "used to" the opposite process. That is why IT specialists expected technical difficulties and decided for replication just in case that one of the disks would fail. This is exactly what happened. It would be possible to call an external company to recover the failed disk, however in a situation when hospital is out of order, time is a very important commodity and a duplication of recovery was the right decision.

On Thursday, 12 December 2019, all IT elements were disconnected from the primary network and approx. around 10.00 in the morning NUKIB analysed the situation and provided recommendations for the recovery plan to renew the infrastructure. The first data for analysis were transferred to NUKIB and isolated networks for DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), ESET and server back-up were installed. NUKIB conducted network and forensic analysis to reveal the scope of infection, persistency of the malware and indicators of compromising, which were immediately distributed to other organizations and in fact prevented similar infection (the subject is not mentioned by NUKIB).[50] During the evening, the response team resolved some issues with SYNOLOGY disks and started making bit copies of the disks. During the night, it was decided, based on recommendation and consultation with NUKIB, that DC[51] would be initiated after the analysis made by NUKIB, the response team would wait for SYNOLOGY bit copies and then restore back-ups in the isolated environment and clean servers. The debate was about the necessity of reinstalling all clients. The disk array capacity of the hospital was approx. 60 to 80 TB, where a larger share (around 80%) are PACS (Picture Archiving and Communication System) data, stored elsewhere, so they were not encrypted. Some of the end stations were encrypted but some remained not. However, end stations were not so important because valuable data are not stored there.

[49] Ibid.
[50] NUKIB, ref. 14.
[51] Refers to "Direct Current", which is used by the computer to power electronic components.

On Friday, 13 December 2019, the work was dedicated to the back-up and end stations which were reinstalled. The data restoration in the isolated secure environment took place. A new firewall was set up to block all traffic unless approved by administrators. The separated infrastructure was finished including the segmentation and the copy of the SYNOLOGY disk was finished. During the evening, the team was resolving issues such as 1) back-ups according to the priories set in the recovery plan; 2) there was also the issue of a new server installation and data recovery; and 3) the issue of all PC reinstallation and change of the SSD disk.[52] The decision to make a new installation on a new SSD was taken just in case that some important data on the old disks remained and would be later needed. However, here we faced another problem: Who will deliver approx. 400 or 500 SSDs on Friday? The problem was solved together with Alza.cz which provided supplies. On this day, also the "Next Generation" firewall arrived so it was possible to start building up the security infrastructure. It is important to note that the firewall is the key element also in the case of fragmentation – fragmentation was done also before the incident; however, it was limited due to the firewall construction. The new firewall thus unlocked new possibilities.

During the weekend between 14 and 15 December 2019, the response team continued the work on back-ups and end stations. Back-ups were copied and disks rebuilt, end stations were reconstructed, and infrastructure restored. End stations were designed for local use. This means that some stations were equipped with the PC, printer and MS Word in advance and other worked properly but without connection to the central network. This was in fact very frequent misinformation in media that devices were not working. This was not true as they were working, but they were accessible only locally.

However, the most important day was Monday 16 December (Day D) because NUKIB gave recommendation to install a new domain. It was a crucial decision, which basically meant starting on a "green field". Before this recommendation, the IT department of the hospital expected that the existing back-up would be used and the system would be restored from it in a time horizon of two or three days until full recovery. However, NUKIB advised that all back-up shall be treated as "infected" until it the exact time when virus penetrated the system would be known. This itself was a very consuming activity (which eventually lasted one month). Thus, decision to start on a "green field" was a rational approach, although it complicated restoration works. It was a big dilemma because some disks were fully infected while other were just partly encrypted and there were two ways: first, to proceed piece by piece; or second, to consider everything infected.

After the analysis of logs, the IT department decided to follow the recommendation of NUKIB and start a fully new domain. It means that four days after the attack took place the new domain driver was installed in a clean network and all servers were newly installed. Old servers, which were considered uninfected, were locked into the quarantine network and data from there were extracted, verified for infection, collected, cleaned and imported into the new system. This part was quite time consuming. It means that back-ups were not used in a direct and proper way because everything was newly set up and cleaned. The lesson learned here is to have a separate back-up of data and a separate

[52] Refers to "Solid-State Drive", which is basically a storage device containing non-volatile flash memory.

back-up of the station itself to be prepared for a quick restoration. When there is break down of the server, then it is possible to restore the server from the virtual setting.

NUKIB also approved the back-up recovery plan with a new server with a recommendation not to use the old server except data. NUKIB also approved VPN clients via SOPHOS (allowing two level authorization, which is positive for connecting external companies) and approved data recovery from the server – file share. During Monday, basic policy domains were set up together with the connection to the back-up on a new hardware. On Monday, reconstruction of priority servers started, using new installation and data migration. These servers included FEIS for economy, FLUX for human resources, PACS for visual documentation, LEKIS for pharmacy, and critical STAPRO FE for the health system. The renovation dealt also with the DC, WSUS (Windows Server Update Services), ESET, DLP (Data Loss Prevention) and other service servers.

To sum up, the attack was very effective because it succeeded in penetrating into the system without previous detection, managed to encrypt the data and resulted in severe restrictions in the provided health services. The hospital was "totally blind" for one week. On the other hand, no data were lost or stolen and the hospital relatively early managed to restore systems without paying any ransom. It is necessary to highlight that the key systems were restored within five days since the recommendation of NUKIB to create a new infrastructure. Moreover, security advices of NUKIB were followed. The response to the attack was relatively well managed. During the first five days, the IT response team in cooperation with an external company and NUKIB succeeded in the initial analysis of the attack, securing and multiplying the back-up and preparing restoration works. Based on the analysed data, the final decision was made five days after the attack that renovation would start at the green field. Rough timeline and activities are summarized in Table 1.

Table 1: Timeline of the first five days

Wednesday, 11 December 2019
2:50 "Good evening, our application is not working well"
3:10 Ad locum analysis of the problem (STAPRO FE problematic update revealed)
3:13 STAPRO FE support contacted
3:30 Crypto virus infiltration suspected (physical disconnection of infrastructure)
4:00-5:00 IT team meets with external company, minimal physical infrastructure
5:00-8:30 Emergency Task Force meeting & relevant partners and authorities, finally NUKIB is contacted
8:30 Samples of encrypted data given to the Police
10:00 First logs sent to ESET for analysis
13:00 ESET laboratory conducted activities
14:00 NUKIB analysed problem and issued recommendations
20:30 Conservation of infrastructure, waiting for log analysis, thinking about duplication of recovery

Thursday, 12. 12. 2019
7:00 Physical disconnection of all IT elements from primary network
10:00 NUKIB recommendations and analysis, provided data for analysis and recommendations for recovery + installations of isolated networks
20:00 SYNOLOGY disk problem – bit copy initiated
Until 1:00 Working on recommendations from NUKIB (DC after analysis on Monday; wating for bit copy; after that server cleaning in isolated environment and reinstallation of all clients)
Friday, 13. 12. 2019
7:00 Back-up and work on end stations (SYNOLOGY back-up finished; data recovery into isolated environment; reinstallation of clients; set up of new firewall that blocks everything; separation of infrastructure and segmentation)
22:00 Recovery according to priorities (recovery plan), necessary installation of new servers, reinstallation of all PCs and exchange of all disks for SSD
Weekend 14. and 15. 12. 2019
Copying data from recovery, rebuild of disks, reinstallations of end clients, renewing infrastructure, enabling use of end stations in local use.
Monday 16. 12. 2019 (Day D)
New installation of key systems (data migration only)
FEIS for economy, FLUX for human resources, PACS for data visualization, LEKIS for pharmacies, STAPRO FE for health documentation + service servers

Source: Authors.

Mid-term Response and Recovery

On Tuesday, 17 December 2019, clients were installed together with PACS – ICZ servers and preparations for primary network set up were made. NUKIB contributed with policy set up of the DC and approved the back-up method. In the following days, works on the client installation continued, including STAPRO and connected modalities like CT (Computed Tomography), MR (Magnetic Resonance), DR (Diagnostic Radiology) to the PACS sever, enabling sharing virtual images. The key activity was launching the RTG (Radioisotope Thermoelectric Generator) after the security control and gateway modality for RTG. This is very important, because when RTG is working, then you can open hospital for customers. Soon, FEIS and FLUX servers were installed together with the viewer for DICOM PACS – ICZ and PACS modality was extended with ultrasound. On Friday, 20 December, installation of clients continued and the STAPRO server was launched together with LEKIS for pharmacies – allowing to issue prescription. It means that the performed changes enabled doctors to work in a proper way. To sum up, the response team succeeded in restoring the main systems in five days and reinstalling approx. 400 computers out of 600. New server environment was created and network infrastructure was optimized. This was a challenge because there are dozens of companies requiring

access into the system, so it is necessary to set up some security policy for these external partners.

Before the end of 2019, several additional activities were conducted. Before Christmas, VPN via Firewall was launched, installation of clients continued and works on the stabilization of the system were conducted. Some breaking point was the launch of laboratories including connections and restoration of bed departments and ambulances (until then, laboratories were operating but were disconnected). Here, a very important lesson is related to the sort of "euphoria of the users". When one user sees that their part of the system is in operation, other users start to be more demanding with a tendency to give individual instructions to the members of the IT team. Despite the fact that the users might be high ranked respectable people within the hospital, it is worth to strictly follow the recovery plan and set up priorities, otherwise an individual task for team members might undermine the performance of the team. In other words, users shall be patient and not misuse their privileges and think that their department is the most important and deserves special attention. The solution might be to create a priority list, which will be flexible and reflect power of individual department managers, senior doctors, etc.

At the end of 2019, almost three weeks after the attack, the hospital was operational. Internal hospital departments were re-opened and e-mails of the doctors were renewed. However, renewing all applications and program took several weeks more.[53] As of mid-January 2020, the damage was estimated at 38 million CZK (approx. 2 mil USD) due to limited healthcare services and another 2 million CZK (approx. 100,000 USD) was needed for the reinstallation of servers.[54] However, in fact, the calculation of damage is a very complex and challenging task. Calculations usually include operational loss, including the loss of profit, together with costs needed for the IT infrastructure restoration. However, both areas are problematic. For example, some operations might be postponed and restoration of the IT infrastructure involves costs which were generated over time due to lack of previous investment.

It is important to note that NUKIB was not the only cooperating actor. Crisis managers cooperated also with data officers from other hospitals. In this case, synergic cooperation was created with data officers from Prague IKEM, Faculty Hospitals in Olomouc and Hradec Králové and Na Bulovce hospital in Prague. The cooperation contributed to minimalizing costs for maintaining security and sharing knowledge as other IT officers asked what happened and how to avoid the attack.[55] Despite showing solidarity, the response and support might have been bigger, especially in the area of knowledge exchange. There are some individuals who are pushing for better cooperation, however here the human factor is important. Small hospitals do not have the capacity to pay for an IT security specialist and these experts soon leave for the private sector. And from the other perspective, this person would not have a good overview of what is going on in different parts of the country. There are many private organizations doing that. However, there is some project by the Central Bohemian Region, which is preparing to set up a team of IT experts who will help. The project might bring benefit for regional hospitals, which will have a network with an early warning mechanism, exchange of data and good practice.

[53] CT, ref. 31.
[54] CT24, ref. 33.
[55] SHABU, ref. 41.

2020 brought new challenges. During the first week, ambulances became operational together with the technical and economic services. The file server, mail server and internet were launched. Despite one year since the incident, some minor parts of the system were not restored. The reason is that existing applications installed years ago were out of the date and the producers or providers did not provide updates or installation sets anymore. That is why in Benešov, one year since the attack, the web part of the intranet is not finished yet along with the web part of the personal system – the user upgrade, which is now in the testing phase. The intranet will be resolved next year and will be most probably externally based. As of 20 January 2020, approx. 70% of the systems were online, however, some systems including the blood bank or nutrition were still out of order, which created some side effects: there was no blood collection during the event resulting in lack of blood, thus, the hospital had to buy reserves elsewhere.[56] These problems were also soon overcome.

As a result of the attack, the Benešov hospital got a new infrastructure involving a new firewall, which opened new opportunities for the management of the security infrastructure. Active management of the network allowed a higher level of segmentation and VPN was put behind the firewall. The server environment is characterized by a fully new virtual environment. All servers are running on the new hardware and new servers were fully installed in clean environment. Data loss protection was enriched by a new level and the hospital now uses two SYNOLOGY back-ups. As prior to the Ryuk attack, end stations were equipped with Windows 10 and secured with a new data loss prevention policy. Devices were equipped with Windows 7, Windows 10, Embedded, with 2 Windows XP devices not connected to the network. However, the server system has become much more balanced and the virus brought about the opportunity to change many things which would be difficult to change when operating. Today, the hospital is equipped with IT technologies which are able to detect anomalies in the network or at the end stations.

LESSONS LEARNED

To draw lessons learned from the case is not an easy task. This is mainly due to the fact that this article analyses one single case: the reaction of one hospital to one specific attack. In reality, the threats of cybersecurity are very complex and so is the internal environment of hospitals, which differs in the level of IT security, material equipment, capacities, etc. For this reason, recommendations can be formed only at certain level of generalization, which is however attitude of the majority of articles and this one is not an exception. Nonetheless, "micromanagement" presented in the second chapter may provide valuable information about the crisis response to the security incident, which is (hopefully) also partially applicable in other organizations and which might accompany the following recommendations.

In order to close holes in the cheese, some preventive measures influencing organizational factors are necessary. Organizational factors, however, are the key to an effective response. For this reason, this part brings several ideas to set up and develop preventive and responsive measures. Kučínský and Sikora mention 7 general preventive measures including: 1) Data back-up outside of the system (offline); 2) Monitoring, 3) Segmentation

[56] Ibid.

of the network, 4) Software updates, 5) Removing dangerous access; 6) User training, 7) Macro features in MS Office. Regarding the reaction, both authors mention: 1) Necessity of work continuation, 2) Communication strategy, 3) Communication with authorities.[57] Their summary of measures is logical and may be generally applied to any institution. For this reason, it has also provided the inspiration for the systemic approach presented in Chart 2.

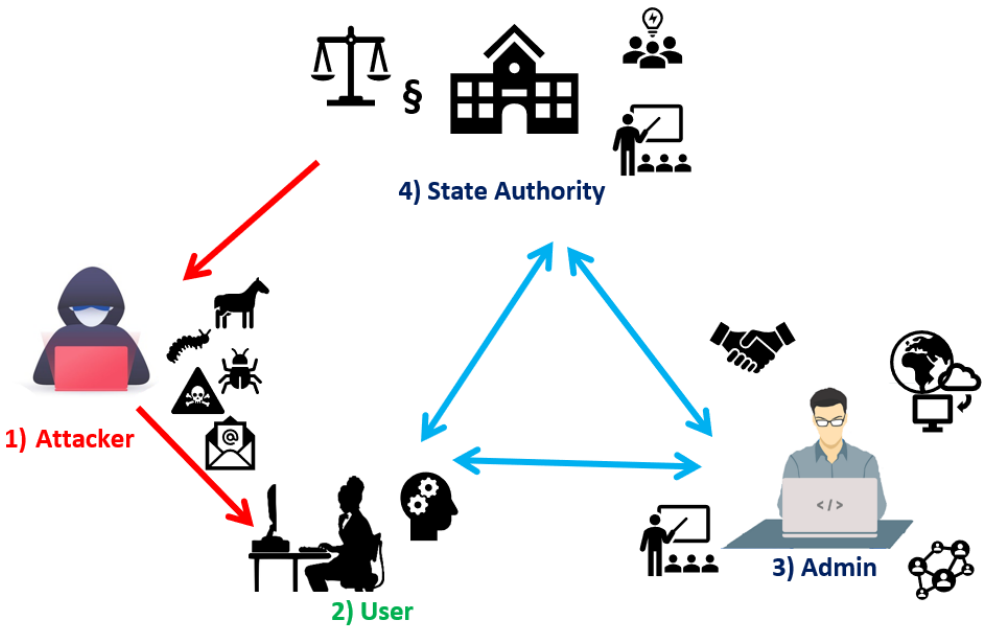
In the mentioned schematic in Chart 2, there are four principal actors including the attacker, user, IT administrator, and state authority. Like any schematic, it simplifies the reality because in fact there is no single state authority and usually there are multiple users and sometimes also multiple attackers. However, it is possible to distinguish four key roles and other actors might be subordinated in the categories.

An attacker entering into the system may be considered as independent variable. Regardless of their motivation, attackers try to penetrate the system, usually via exploitation of gaps in the IT platforms operated by users. In this sense, users are a very wide and diverse category ranging from e-mail users to service consumers or providers. They may work in private or public domains.

The first important measure is to keep users aware and vigilant about current trends and promote safe behaviour in the online space. Attackers often abuse users' curiosity, greed or fear. This is especially the case of phishing or spear phishing and sextortion attacks. However, ICT skill development is a long-term process, which faces many educational challenges.[58] Due to the anthropocentric nature of the cyber-security threats, human factor plays an important role in avoiding attacks and the appropriate level of skills may decrease its incidence. Another important measure regarding users is to let them work in a safe environment, which partly depends on the approach of administrators. Every workstation requires its specific security level. The higher potential loss, the higher preventive measures shall be taken. A minimum standard is a good firewall, updated antivirus programme or other software detecting potential malware or spyware. In many cases, problems are associated with personal e-mail and VPN access. That is why administrators shall consider ban of personal emails and restrictions on VPN access. Users might be significantly affected by the attack and thus should be prepared for prospective changes. The cyberattack may lead to the "set back in time". Instead of computers, doctors will have to use paper and pen again and call the laboratory for results which are not displayed immediately. This change in the system will be time consuming and decrease effectivity of the system. For this reason, doctors shall be trained for this situation to work in urgent cases without IT support. Regular training and restriction of users is a key and IT department shall not compromise its high security standards by allowing exceptions that make the system porous.

[57] KUČÍNSKÝ – SIKORA, ref. 1, p. 43.
[58] BENEŠ, Pavel – MUDRÁK, David – PROCHÁZKA, Josef – RAMBOUSEK, Vladimír – ŠTÍPEK, Jiří. Research of ICT Education in the Czech Republic. *Problems of Education in the 21st Century*, 2008, 5(1), 24–34.

Chart 2: Systemic diagram of civil dimension of the cybersecurity



Source: Authors

Due to their closeness to the users and their expert skills, administrators play central part in the system. For this reason, they are the best people to inform about the current trends in the IT security and provide training to the users. They ensure ad locum security of the IT devices (protection of end stations) and are responsible for data back-up (offline back-up). IT administrators shall restrict the access to privileged admin accounts and keep exceptions on a minimal level. Standard is a good firewall, automatic management of network operations and micro segmentation of the network. These are the key actors in communication with state authorities. Due to their access and overview of the systems, they provide the necessary data allowing complex analysis of the IT domain including incident notification and reporting. During the incident, administrators stand in the front line to prevent or minimalize the damage. For this reason, administrators have rich and diverse experience, which is worth sharing via networks with other administrators and institutions. Finally, administrators play the most important part in cooperation with state cybersecurity authorities in responding to events, as Cyber Security Response Teams (CSIRTs) may help in the initial defence or in later stages with incident investigation and data restoration.[59] Especially frequent, regular and complete data back-up at safe location seems to be the key aspect of minimalizing damage. During the restoration, administrators shall keep in mind the motto: "Clean installation required". It is an unfortunate practice that admins use back-ups without changes and cleaning the network.

[59] PAČKA, Roman. *CSIRT: V přední linii boje proti kybernetickým hrozbám*. Brno: CDK, 2019.

Because virus can hit any time, it is good not to address too many projects at one time and stay focused to a limited number of issues.

Next to the above-mentioned tasks of the national authority, there is a significant role in providing regulatory standards. These include basic ICT laws and key aspects of crisis management in relation to cyber security incidents. Cybersecurity also has an important criminal dimension with implications for post-incident proceedings, which is one of the most challenging parts as the attackers are rarely punished in accordance with law.[60] Due to the power of national authorities, their capacity and relation to other executive branches, national authorities play an important role in cybersecurity defence. For this reason, their representatives shall be included in the policy making bodies and closely cooperate with other relevant institutions including concerned ministries and stakeholders. State authorities may greatly contribute to information exchange and education process regarding the relevant cybersecurity IT skills. Organized events may support security in both private and public spheres. The legal dimension of cybersecurity is evolving very fast at the national and international level as well. Complexity of the legal system is sometimes hard to understand for IT experts and vice versa.[61] Moreover, cybersecurity is also specific in relation to different types of stakeholders.[62]

As pointed out by many, the key for the success is to enhance preventive measures. This may include areas of client identification and authentication, capacities of network resilience, cyber intelligence, surveillance and reconnaissance or cyber early warning and response.[63] Special attention shall be paid to critical infrastructure. The progressing COVID-19 infection shows that hospitals are an inseparable part of the critical functioning of the state. Also, the new pandemic creates stronger pressure on cybersecurity of healthcare.

Another necessity is to work together. From the IT perspective, all hospitals are the same and work with same kind of data: PACS, Human Resources, Finances, etc. The environment is not homogenous but has many common features and challenges for IT specialists in hospitals. Fortunately, there are many qualified teams in the Czech Republic, including people from NUKIB or DPO. which is also centralized to some degree, but there is absence of SOC – someone who will coordinate the security of hospitals in the Czech Republic. It is necessary to encourage people who are fans of the IT, rather than desk managers with restrictive and repressive attitude. It is also necessary to keep the hospital management informed about IT developments and threats. When the managers are informed and educated in the IT, they put higher priority to the IT agenda. Many small

[60] POLČÁK, Radim. Kybernetická bezpečnost jako aktuální fenomén českého práva. *Revue pro právo a technologie*, 2015, 11(6), 95–149.
[61] HROMADA, Martin – HRŮZA, Petr – KADERKA Josef – LUŇÁČEK, Oldřich – NEČAS, Miroslav – PTÁČEK, Bohumil – SKROUŠA, Leopold – SLOŽIL, Richard. *Kybernetická bezpečnost – teorie a praxe*. Brno: Powerprint, 2015.
[62] BERNÁTEK, Josef. Kybernetická bezpečnost řepařského a cukrovarnického sektoru. *Listy cukrovarnické a řepařské*, 2019, 135(11), 375–376; BERNÁTEK, Josef. Kybernetická bezpečnost chemického průmyslu v České republice. *Chemické listy*, 2020, 114(4), 295–298; ANDRAŠKO, Josef. Bezpečnosť informačných systémov verejnej správy vo svetle zákona o kybernetickej bezpečnosti a zákona o informačných technológiách vo verejnej správe. *Revue pro právo a technologie*, 2019, 10(20), 3–40.
[63] VASILESCU, Cezar. Kybernetické útoky: nové hrozby pro kritickou informační infrastrukturu ve 21. století. *Obrana a strategie*, 2012, 12(1).

organizations think that cybersecurity is not their issue, but this might be caused by the fact that they cannot detect the threats. Moreover, attackers will be always one step ahead and there will always be enterprises with lack of funds or lack of people who will be able to ensure high level of security – to have everything up to date and provide support to the users.

Hospitals shall consider IT audits, which are a double-edged weapon. Some are made for the purpose of matching formal criteria. It is much better to create a team of IT specialists in each hospital, who will visit the participating hospitals to have a look at the security. IT audits are valued when conducted by skilled people who know what to look for and what are the highest standards of IT security. It is also possible to consider insurance of the services. However, here the issue is that insurance companies require a high standard of protection (based on the recommendations of NUKIB) – and in this case there is low probability of a successful attack. When the standard of protection is not high, then the insurance is so expensive that it is better to invest money directly into the IT. However, insurance might play important role in the future, as the number of attacks increases.

One general rule can be applied in the communication. As shown in the case of the Benešov hospital, communication is key for preventing further damage. There is nothing wrong to admit that you have been attacked and you are asking for help. That is why it is good to openly share information with other regional hospitals, state hospitals, NUKIB, data protection officers or rescue services. It is good to share good practice and lessons learned. Lastly, it is worth to promote solidarity among hospitals because cyberattack may affect any of them. Facing a large-scale incident is a very stressful situation for patients, doctors, hospital mangers and last but not least the IT response team who performs the recovery and works to put things in a proper order. That is why it was surprising that the public expert debate regarding the incident in the Benešov hospital was very critical and that the criticism was very normative – applying very high standards on the hospital without being aware of its resources and possibilities.

CONCLUSION

The case of the Benešov hospital is not unique in the global context as every day hospitals face the challenge of ransomware. The prospects are not very positive as hackers are hidden beyond the curtain of anonymity and there are no physical borders in the cyberspace. Despite cyberattacks being considered illegal, hackers are rarely discovered, prosecuted and punished. Due to low efficiency of rule of law enforcement, emphasis on preventing the cyber-attacks offers more prospects.

This article was dedicated to the analysis of one large-scale incident which happened a year ago in the middle-sized regional hospital, which might be labelled as an “average hospital” in many aspects. This was also the case of its IT infrastructure, which faced an unprecedented attack. Despite all security measures including trained personnel, firewall, antivirus, updates, network fragmentation or regular offline data back-up, crypto virus succeeded to cause damage. Despite data were not stolen or destroyed, limited operation of the facility led to loss in millions of Czech korunas. This article provided overview of main organization factors before and after the attack. These overviews might be well placed into the model of Swiss cheese. Unfortunately, for good

reason, some data are not public. This limits the application of the Swiss cheese model. However, the authors believe that examination of this case brought interesting information to fellow readers and provided lessons learned.

The principal research question: "What organizational and security factors contributed to good management in the post-attack period?" has a very complex answer. As the second chapter showed, the management would be not possible without a response team of IT specialists who know what to do. It would be not possible without data back-up as well as without the help of NUKIB or consultations with an external IT security company. Management of the hospital acted exemplary in order to prevent further losses and tragedies due to limitation of healthcare services. Communication between the IT response team, NUKIB and management of the hospital was of key importance. Despite unprecedented loses, Ryuk opened new possibilities to improve the IT security infrastructure and harmonize the environment. It also contributed to incorporation of new security elements into the system.

The article also revealed also some systemic "imperfections". There is absence of some platform which will contribute to the exchange of good practice and management of security operations in real time. Despite the fact that NUKIB provided professional guidelines and its recommendations were followed, there is absence of some sort of IT Security Operation Centre (SOC) – a facility where IT systems of hospitals will be monitored, assessed and defended. Some imperfections can be addressed internally: not to compromise high level of security with exceptions and ease of restrictions regarding rights of user or VPN connections.

Despite all attempts, this article has some inherent limits. First, the vector of the attack is not fully known so far, which prevented deeper analysis. This also had an impact on the second issue: the application of the "Swiss Cheese" concept, which was used as a source of inspiration, rather than a fully operable analytical tool. And third, due to a very complex nature of cyber security threats on one side and high variability of organizations, the third chapter formulated rather general recommendations with universal applicability. Nonetheless, authors hope that the second chapter provided unique insight into "micromanagement" of a security incident, which might provide good inspiration for other organizations, not only in healthcare.