ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA BIOMEDICÍNSKÉHO INŽENÝRSTVÍ

Katedra zdravotnických oborů a ochrany obyvatelstva

Kybernetický útok v prostředí poskytovatele zdravotnických služeb

Cyber Attack in the Environment of the Healthcare

Bakalářská práce

Studijní program:	Ochrana obyvatelstva
Studijní obor:	Plánování a řízení krizových situací
Autor bakalářské práce:	Lenka Pardamcová
Vedoucí bakalářské práce:	PhDr. Lukáš Miklas, MBA

Kladno 2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení:	**Pardamcová**	Jméno:	**Lenka**	Osobní číslo:	**500041**
Fakulta:	**Fakulta biomedicínského inženýrství**				
Garantující katedra:	**Katedra zdravotnických oborů a ochrany obyvatelstva**				
Studijní program:	**Ochrana obyvatelstva**				
Studijní obor:	**Plánování a řízení krizových situací**				

II. ÚDAJE K BAKALÁŘSKÉ PRÁCI

Název bakalářské práce:

Kybernetický útok v prostředí poskytovatele zdravotnických služeb

Název bakalářské práce anglicky:

Cyber Attack in the Environment of the Healthcare Service Provider

Pokyny pro vypracování:

Bakalářská práce bude pojednávat o kybernetických útocích na nemocnice. Jejím předmětem bude analýza současného stavu úrovně zabezpečení informačních systémů nemocnic v ČR proti kybernetickému útoku. Teoretická část bude obsahovat vymezení základních pojmů, popis legislativního rámce a specifikaci kybernetického ohrožení zdravotnických zařízení. Na základě rešerše odborné literatury bude cílem identifikovat zranitelná místa a navrhnout možná řešení zvýšení úrovně kybernetické bezpečnosti. Součástí práce bude několik vybraných případových studií z českého i zahraničního prostředí. Na základě těchto studií a výzkumu současného stavu úrovně zabezpečení budou demonstrována opatření, jejichž dodržování může snížit jak pravděpodobnost, že bude útok úspěšný, tak snížit pravděpodobnost vyšších škod u již proběhlého útoku. Bakalářská práce bude zpracována ve spolupráci s Ústřední vojenskou nemocnicí – Vojenskou fakultní nemocnicí Praha.

Seznam doporučené literatury:

[1] SEDLÁK, Petr a Martin KONEČNÝ. Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru, Brno: CERM, akademické nakladatelství, 2021, 429 s., ISBN 9788076230682
[2] PAČKA, Roman, CSIRT: v přední linii boje proti kybernetickým hrozbám, Brno: Centrum pro studium demokracie a kultury, 2019, ISBN 978-80-7325-473-5
[3] KOLOUCH, Jan a Pavel BAŠTA, CyberSecurity, Praha: CZ.NIC, z.s.p.o., 2019, ISBN 978-80-88168-31-7

Jméno a příjmení vedoucí(ho) bakalářské práce:

PhDr. Lukáš Miklas, MBA

Jméno a příjmení konzultanta(ky) bakalářské práce:

Datum zadání bakalářské práce: **14.02.2023**
Platnost zadání bakalářské práce: **20.09.2024**

doc. Mgr. Zdeněk Hon, Ph.D.
vedoucí katedry

prof. MUDr. Jozef Rosina, Ph.D., MBA
děkan

PROHLÁŠENÍ

Prohlašuji, že jsem bakalářskou práci s názvem Kybernetický útok v prostředí poskytovatele zdravotních služeb vypracovala samostatně pouze s použitím pramenů, které uvádím v seznamu bibliografických odkazů.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

V Kladně dne 17.05.2023

…….
Lenka Pardamcová

PODĚKOVÁNÍ

Touto cestou bych ráda poděkovala mjr. PhDr. Lukáši Miklasovi, MBA za ochotu, trpělivost a cenné připomínky při vedení této práce. Dále bych poděkovala všem respondentům, kteří si udělali čas a zúčastnili se rozhovoru.

ABSTRAKT

Hlavním náplní bakalářské práce bylo mapování současného stavu ochrany nemocnic před kybernetickými útoky formou vedení strukturovaných rozhovorů s odborníky na tuto problematiku přímo z vybraných zdravotnických zařízení.

V rámci teoretické části této práce byl utvořen přehled legislativních předpisů upravujících probíranou problematiku jak v rámci České republiky, tak i v rámci Evropské unie. Tato část se dále věnuje vymezení základních pojmů, které se v oblasti kybernetické bezpečnosti běžně vyskytují, a s kterými i tato práce dále pracuje. Teoretická část je věnována také popisu kritické informační struktury, specifik kybernetického ohrožení zdravotnických zařízení a v neposlední řadě také krátkému popisu kybernetických útoků, které se odehrály na území České republiky a obdobných útoků, které se udály v zahraničí.

Ve výzkumné části bylo provedeno několik strukturovaných rozhovorů s odborníky z prostředí nemocničních zařízení, kteří se této problematice věnují ve své organizaci. Informace získané v rozhovorech byly následně vyhodnoceny metodou interpretativní fenomenologické analýzy a využity pro vytvoření uceleného pohledu na současný stav ochrany nemocnic před kybernetickými útoky.

V závěru práce byla identifikována rizika pro zdravotnická zařízení z pohledu kybernetických útoků a na základě této identifikace byla navržena možná opatření ke zlepšení současného stavu v této oblasti.

Klíčová slova

Kybernetický útok; zdravotnické zařízení; bezpečnost; analýza; malware

ABSTRACT

The main content of the bachelor thesis was the mapping of the current state of protection of hospitals against cyber-attacks in the form of conducting structured interviews with experts on this issue directly from selected healthcare facilities.

As part of the theoretical part of this work, an overview of the legislative regulations governing the discussed issue was created both within the Czech Republic and within the European Union. This part is also devoted to the definition of basic concepts that are commonly found in the field of cyber security and with which this work continues to work. The theoretical part is also dedicated to the description of the critical information structure, the specifics of the cyber threat to medical facilities and, last but not least, a brief description of cyber-attacks that took place in the Czech Republic and similar attacks that took place abroad.

In the research part, several structured interviews were conducted with experts from the environment of hospital facilities who deal with this issue in their organization. The information obtained in the interviews was subsequently evaluated using the method of interpretive phenomenological analysis and used to create a comprehensive view of the current state of hospital protection against cyberattacks.

At the end of the work, the risks for medical facilities from the point of view of cyber-attacks were identified and, based on this identification, possible measures to improve the current situation in this area were proposed.

Keywords

Cyber crime; Health Care Provider; Security; Analysis; Malware

Obsah

1 ÚVOD

Tato práce se zabývá problematikou kybernetické bezpečnosti se zaměřením na kybernetické útoky vedené na zdravotnická zařízení, zejména nemocnice. V práci je uveden přehled legislativních předpisů upravujících diskutovanou problematiku jak na národní úrovni, tak v rámci Evropského společenství. Teoretická část práce je dále věnována vymezení základních pojmů běžně se objevujících v této oblasti a také popisu kritické informační struktury, specifik kybernetického ohrožení zdravotnických zařízení a v neposlední řadě také krátkému exkurzu do předchozích kybernetických útoků vedených na české nemocnice a dále obdobných útoků, které se udály v zahraničí. V rámci praktické části bakalářské práce byla provedena série rozhovorů s odborníky na problematiku kybernetické ochrany nemocnic, ze kterých bude vyvozen současný stav na poli ochrany nemocnic před kybernetickými útoky.

Téma kybernetických útoků na zdravotnická zařízení je v současné době velmi diskutováno, zejména v důsledku již proběhlých kybernetických útoků na nemocnice v České republice. Důvodem ke zvolení tohoto tématu bakalářské práce je můj dlouhodobý zájem o legislativu a právní předpisy. Kybernetický útok je trestným činem stejně tak, jako např. fyzické napadení, tudíž se jedná o legislativně upravovanou oblast. Zároveň se jedná o poměrně novou oblast kriminality, která přišla společně s moderní výpočetní technikou. Masivní rozvoj výpočetní techniky za poslední desetiletí s sebou nevyhnutelně přináší i nový prostor pro kriminální činnost a jednou z těchto nových kriminálních činnosti jsou právě kybernetické útoky.

Od této práce se očekává, že přinese ucelený pohled na problematiku kybernetické bezpečnosti s detailním zaměřením na ochranu zdravotnických zařízení (nemocnic) před kybernetickými útoky a zmapuje současný stav na poli této oblasti.

2 CÍLE PRÁCE

Hlavním cílem této práce je identifikace zranitelných míst a navržení postupu či doporučení, které mohou zabránit kybernetickému útoku na zdravotnické zařízení, případně snížit závažnost jeho dopadů. Práce si však současně neklade za cíl stanovení konkrétních technických detailů v procesu zabezpečení informačních a komunikačních systémů.

Za účelem dosažení vytýčeného cíle se teoretická část zabývá legislativními předpisy souvisejícími s kybernetickou bezpečností, a to jak předpisy národními, tak předpisy evropskými. V teoretické části hledá práce také odpověď na otázku, jaké specifické znaky má kybernetický útok vedený na zdravotnické zařízení, a proto kromě legislativního rámce uvádí a definuje vybrané pojmy z oblasti kybernetické a informační bezpečnosti, stejně jako z oblasti kritické informační infrastruktury.

Těžištěm práce je poté část praktická, jejímž cílem je na základě rozhovoru s odborníky ve vybraných nemocnicích zabývající se kybernetickou bezpečností zmapovat současný stav, ale zejména limity či nedostatky kybernetické bezpečnosti v tomto prostředí. Dílčím cílem je proto formulace relevantních otázek, týkajících se zajištění kybernetické bezpečnosti ve zdravotnickém zařízení Na základě analýzy rozhovoru, studiem rešerše a případových studií budou popsány problémové oblasti a navržena opatření.

3 PŘEHLED SOUČASNÉHO STAVU

3.1 Legislativní rámec

Kapitola „Legislativní rámec“ má za cíl představit základní právní dokumenty, které se zabývají kybernetickou bezpečností (dále jen „KB“). Tak jako veškerá činnost a fungování v reálném světě je nějakým právním způsobem upravováno, i fungování v kybernetickém prostoru musí být regulováno právem, aby nedocházelo k protiprávnímu jednání, byla zajištěna bezpečnost či byla stanovena práva a povinnosti subjektů, kterých se týká kybernetická bezpečnost [34].

3.1.1 Zákon o kybernetické bezpečnosti

Hlavním zákonem, který se v České republice (dále jen „ČR“) týká KB je zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, obecně známý jako zákon o kybernetické bezpečnosti (dále jen „ZKB“). Tento zákon, účinný od 1. 1. 2015, upravuje práva a povinnosti osob, ale i pravomoc a působnost orgánů veřejné moci na poli kybernetické bezpečnosti [3]. Zákon vychází z předpisů Evropské unie (dále jen „EU“) a jeho účelem je zajištění bezpečnosti informačních systémů (dále jen „IS“). Zákon vymezuje základní pojmy, které se týkají KB. Tento právní předpis také zavádí hlášení těchto incidentů a upravuje navazující opatření, kterými lze na kybernetické bezpečnostní incidenty reagovat. Tento předpis však neplatí pro informační nebo komunikační systémy, které zpracovávají utajované informace [2, 3].

Zvláštní zřetel je v zákoně brán na prvky kritické informační infrastruktury (dále jen „KII“) nebo na systém prvků kritické infrastruktury (dále jen „KI“) a na povinnosti, které je povinen provozovatel informačního systému KI povinen dodržovat [2].

Zákon také pamatuje na povinnosti skupiny CERT (z anglického Computer Emergency Response Team) [5]. Tento tým informuje o známých zranitelnostech a poskytuje technickou podporu při narušení zabezpečení na národní úrovni. Úkolem týmu CERT je působit jako prvotní zdroj bezpečnostních informací nejen pro orgány státu, ale i jiné organizace a občany [35].

Zákon také zavádí pojem „stav kybernetického nebezpečí“. Dle ZKB je stav kybernetického ohrožení definován jako: „*stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost služeb elektronických komunikací anebo bezpečnost a integrita sítí elektronických komunikací, a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací*“ [2, § 21 odst. 1]. Stav kybernetického nebezpečí může být vyhlášen nejdéle na dobu sedmi dnů a může být v případě potřeby prodloužen. O tom, zda bude vyhlášen nebo prodloužen tento stav rozhoduje ředitel Národního úřadu pro kybernetickou bezpečnost (dále jen „NÚKIB“). Doba trvání stavu nesmí však překročit třicet dnů. Během toho, co trvá tento stav, NÚKIB informuje vládu o postupech řešení kybernetického nebezpečí a je oprávněn vydat rozhodnutí anebo opatření obecné povahy ke zmírnění nebo zamezení následků kybernetické hrozby.

V zákoně je dále pamatováno na kontrolu dodržování povinností provozovatelů služeb elektronických komunikací a jsou zde uvedeny konkrétní přestupky, které mají trestně právní dopady [2].

3.1.2 Směrnice NIS

Směrnicí NIS se rozumí směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Cílem této směrnice je sjednocení právní úpravy pro oblast bezpečnost sítí a IS v rámci jednotlivých členských států

a zavádí jednotný standart požadované KB. Některé povinnosti, které tato směrnice ukládá jsou v ČR již zahrnuty do ZKB. Směrnice NIS však rozšiřuje seznamy povinných subjektů, pro které jsou určeny povinnosti v oblasti ochrany a prevence před kybernetickými útoky (dále jen „KÚ“). Mezi tyto subjekty jsou oproti ZKB zahrnuti provozovatelé základních služeb a poskytovatelé digitálních služeb. Jedná se tedy zejména o cloudové řešení, internetové vyhledávače, ale třeba také online tržiště [3]. Pro účely této práce stojí za zmínku, že povinnými subjekty vycházejícími z této směrnice jsou poskytovatelé zdravotní péče, tedy zdravotnická zařízení včetně nemocnic a soukromých klinik [4].

Další subjekty jako poskytovatele základních služeb pak směrnice NIS přímo definuje pro oblast energetiky, dopravy, bankovnictví, pro infrastrukturu finančních trhů, dodávky a rozvody pitné vody a pro oblast digitální infrastruktury jakou jsou výměnné uzly internetu, poskytovatelé služeb systémů doménových jmen a registry internetových domén nejvyšší úrovně [4].

Jednotlivé členské státy jsou pak zodpovědné za to, aby všichni provozovatelé základních a digitálních služeb přijali vhodná opatření k předcházení incidentům, které ovlivňují bezpečnost sítí a informačních systémů používaných pro poskytování těchto základních či digitálních služeb. Dále jsou subjekty povinny přijmout taková opatření, aby v případě vzniku incidentu, tedy kybernetické hrozby nebo útoku, byly minimalizovány jeho dopady a bylo zajištěno nepřetržité poskytování základní nebo digitální služby. Určené subjekty mají dále povinnost informovat o každém incidentu příslušný orgán nebo tým CSIRT, a to bez zbytečného prodlení [4].

V rámci ČR je týmem CSIRT (z anglického Computer Security Incident Response Team) CSIRT.CZ, jehož agendu vede správce domény .cz sdružení CZ NIC. Cílem tohoto bezpečnostního týmu je řešení a koordinace bezpečnostních incidentů v ČR [5, 36].

3.1.3 Směrnice NIS 2

Směrnice NIS 2, celým názvem Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii, navazuje na předchozí směrnici NIS s několika novými změnami. Oproti předchozí směrnici tato zohledňuje současné trendy, které se týkají kybernetické bezpečnosti. S postupným digitalizováním napříč všemi obory dochází čím dál častěji ke KÚ. Z důvodu častějších útoků došlo ke změnám a vytvoření této směrnice, která by měla právě zajistit lepší kybernetickou bezpečnost v rámci Evropské unie v návaznosti na předchozí KÚ [6].

Největší změnou v této směrnici oproti předchozí směrnici bude rozšíření povinných subjektů (tzv. poskytovatelé regulované služby). Rozšíření je z důvodu, že v dnešní době už není odvětví, které by nepotřebovalo ke svému fungování informační systémy. Proto směrnice NIS 2 klade důraz na zabezpečování systémů poskytující služby společnosti. Směrnice ve svých přílohách č. 1 a č. 2 vyjmenovává, kterých odvětvích se nově vzniklá směrnice týká. V příloze č. 1 nazvané „základní subjekty“ se jedná o následující odvětví:

- energetika,
- doprava,
- bankovnictví,
- zdravotnictví,
- pitná voda,
- odpadní voda,
- digitální infrastruktura,
- poskytovatelé řízených ICT služeb,

- veřejná správa,
- infrastruktura finančních trhů,
- vesmír.

Ostatní služby jsou v příloze č. 2, „důležité subjekty", jimiž jsou:

- poštovní služby,
- odpadní hospodářství,
- chemický průmysl,
- potravinářství,
- výroba,
- poskytovatelé digitálních služeb,
- výzkum.

Jelikož není možné, aby byl každý, kdo poskytuje z jakoukoliv výše vyjmenovaných služeb zařazen do seznamu směrnice je zapotřebí ještě splnit dvě pravidla pro zařazení.

- *„Organizace poskytuje alespoň jednu službu uvedenou v přílohách směrnice, a zároveň:*
- *je středním nebo velkým podnikem, tedy zaměstnává 50 a více zaměstnanců, nebo dosahuje ročního obratu nebo bilanční sumy roční rozvahy alespoň 10 milionů EUR (zhruba 250 milionů CZK)“* [37].

Jsou zde ale výjimky, u kterých nehraje roli, zda se jedná o střední nebo velký podnik. Jsou to služby a organizace, které by při narušení mohly mít závažný dopad na životy a zdraví osob či na veřejný pořádek [6, 37].

Oproti směrnici NIS je kladen větší důraz na zajišťování a zavádění bezpečnostních opatřeních. Za nedodržování směrnice či nezavedení všech nařízených opatřeních budou ukládány vysoké sankce. Samotná vyhláška pak stanovuje výši těchto sankcí: „*nejméně 10.000.000 EUR nebo 2 % celkového celosvětového ročního obratu*“ [6]. Všechny členské státy, což se týká i ČR tuto novu směrnici musí implementovat do své legislativy nejpozději 17. 10. 2024 [6].

3.1.4 Vyhláška o kybernetické bezpečnosti

Vyhláška o kybernetické bezpečnosti byla zveřejněna ve Sbírce zákonů jako Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, zkráceně vyhláška o kybernetické bezpečnosti (dále jen „VKB“). Uvedená vyhláška opět zpracovává směrnici NIS a pro určité subjekty zejména v oblasti KII upravuje například obsah a rozsah bezpečnostních opatření, způsob hodnocení, závažnosti bezpečnostních incidentů v oblasti kybernetické bezpečnosti, způsob a náležitosti pro hlášení incidentu anebo upřesňuje způsob likvidace dat, informací a jejich kopií. Oproti výše jmenovanému zákonu a směrnici určuje tato vyhláška jednotlivé povinnosti při zajištění KB mnohem podrobněji a zachází do větších technických detailů. Jako příklad může být uvedena povinnost určeného subjektu používat nástroj pro správu a ověření identity uživatelů a administrátorů informačního a komunikačního systému, přičemž je dále definováno několik bezpečnostních zásad, které musí nástroj pro správu identit splňovat [3, 7].

3.1.5 Další legislativní požadavky

Aby bylo možné naplnit požadavky již zmíněného ZKB, směrnice NIS a VKB obsahuje právní řád ČR ještě některé další legislativní požadavky. Jedná se zejména o vyhlášku č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, vyhlášku č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, v jejíž příloze je uvedeno devět odvětví a pro každé odvětví konkrétní kritéria pro určení KI [3].

3.2 Vymezení základních pojmů

Tato kapitola se bude věnovat vymezením základních pojmů, které se pojí k dané problematice. Každý obor disponuje svým odborným názvoslovím a není tomu jinak ani v kybernetické sféře. Nicméně vymezení základních pojmů v tomto oboru není vždy jednoznačné, protože definice jsou často nejednotné. V posledních několika letech je však snaha o sjednocení českého názvosloví v kybernetické bezpečnosti [1].

3.2.1 Hacker

Hacker je často nesprávně používaný pojem pro člověka, který se snaží poškodit či narušit systém. Je považován za toho „špatného“, který porušuje zákon. Právě tento člověk se snaží pomoci tím, že proniká do systémů za účelem nalezení slabých míst, odstranění těchto nedostatků a navržení lepšího zabezpečení [1, 16]. Tato metoda simulovaného útoku pro nalezení slabých míst v počítači se nazývá penetrační test. Při tomto „útoku“ nedojde k žádné ztrátě dat či jejích zašifrování. Hacker, který provádí tyto testy se nazývá „etický hacker“ [49].

3.2.2 Cracker

Neboli útočník. Naopak tato osoba je ta, která se s úmyslem dopouští nezákonného jednání. Hledá slabá místa, na která útočí a získává z nich informace. Motivací takového člověka k takovému činu je hlavně vize získání finančního zisku. Na rozdíl od hackera má cracker méně dovedností [1, 16].

3.2.3 Informační systém

Výkladový slovník kybernetické bezpečnosti informační systém definuje jako: *„funkční celek zabezpečující cílevědomé a systematické shromažďování zpracovávání, uchovávání a zpřístupňování informací a dat. Zahrnuje datové a informační zdroje,*

nosiče, technické, programové a pracovní prostředky, technologie a postupy, související normy a pracovníky“ [8, s. 79].

IS primárně slouží ke sběru dat, k jejich ukládání a zpracování, přenosu či k poskytování informací. IS je složen z pěti komponentů, které jsou vzájemně propojeny. Mezi tyto komponenty se řadí software, hardware, data, lidé a proces [38].

3.2.4 Hardware a software

1. Hardware se používá pro označení fyzického vybavení počítače. Např. klávesnice, monitor či pevný disk.
2. Software je naopak nefyzická část počítače, tedy programové vybavení jako například operační systém nebo programy/aplikace [50].

3.2.5 Kybernetický útok

Nejdůležitějším pojmem pro tuhle práci je pojem kybernetický útok. Jak již bylo zmíněno terminologie není jednotná, a ani u tohoto termínu tomu není jinak. Samotný ZKB nedefinuje pojem KÚ, ale pouze kybernetickou bezpečnostní událost a kybernetický bezpečnostní incident [2]. Oba tyto pomy budou dále v práci vysvětleny.

Podle Výkladového slovníku kybernetické bezpečnosti je KÚ definován jako: „*útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků*“ [8, s. 100].

Další definice říká, že kybernetický útok je: „*jakékoli úmyslné jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby*“ [9, s. 82].

Ať už se jedná o jakoukoliv definici všechny mají společný znak a tím je úmyslné jednání [9]. KÚ může provést jak jedinec, tak skupina crackerů. Motivací k provedení takového činu je spousta. Nejčastějším důvodem provést takový čin je vidina finančního obohacení. Při útocích cracker zašifruje data a následně vyžaduje výkupné pro jejich odšifrování. Také velmi často při KÚ dochází ke krádežím cizích dat, které jsou následně prodána. Pokud se data neprodají, dochází k jejich zničení. Dále to mohou být politicky motivované útoky. Kromě zmíněných důvodů to, ale také můžou být útoky vedené na KI, což při narušení může vážně ohrozit fungování a bezpečnost státu [10]. O KI bude pojednávat pozdější kapitola. Dalším velmi typickým znakem útoků je anonymita. Pachatelé KÚ často zůstanou bez jakéhokoliv postihu, protože je obtížné najít místo, odkud byl útok veden [13]. Spousta crackerů, ale i hackerů vystupuje pod různými pseudonymy pro zachování anonymity [14].

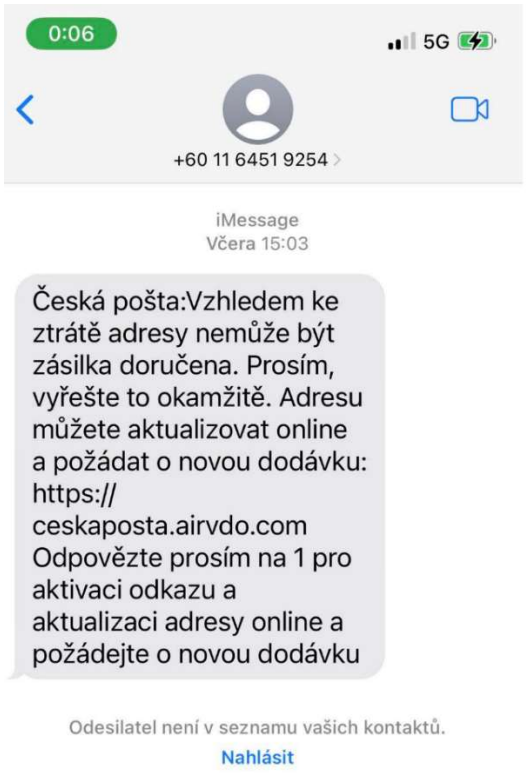
Je důležité zmínit, že jakýkoliv KÚ sebou nese určité následky a dopady. Také je rozdíl, zda útok bude proveden na nějakou firmu, důležitý subjekt nebo jen na jedince. A v neposlední řadě také to, jak moc závažný útok bude. Nejčastějším, ale i nejvýraznějším takovým dopadem je bezpochyby finanční ztráta. U firem a společností se jedná o mnohonásobně vyšší finanční ztrátu než u samotného jedince. Může se jednat o ztrátu přímou, např. ztráta zisku, ale i o ztrátu, která se projeví postupem času. Mezi takové ztráty lze zařadit náklady, které jsou spojené s následnou opravou IS, který byl napaden. Další výdaj je spojen s vylepšením zabezpečení, aby nedocházelo k dalším útokům. Zároveň může dojít i ke ztrátě zisku dlouhodobě, pokud společnost přijde o své zákazníky z důvodu ztráty důvěry. Také zde můžou být započítány různé pokuty anebo peníze vynaložené v soudním řízení. Pokud se všechno toto sečte může to vést ke krachu společnosti [17]. Mezi další dopady KÚ patří ztráta důležitých či tajných dat. Nejzávažnější dopady jsou pří útoku na zdravotnická zařízení a na prvky KII. V takovém případě může dojít i k vážnějším následkům než jen finanční ztrátě. V některých

případech může dojít až k úmrtí pacientů ve zdravotnickém zařízení. Dopad KÚ na jedince ve většině případů nemá takový dopad, jako u společností či důležitých objektů. Pokud byl útok veden na samotného jedince ve většině případů se jedná „pouze“ o menší ztrátu peněz či osobních dat [18, 19].

S neustálým rozvojem doby a nových technologií se rozvíjí i samotné typy KÚ. Na počátku to byly jednodušší útoky, které se postupem času a vývojem informačních a komunikačních technologií staly složitější. V dnešní době je známo mnoho typů KÚ, z nichž zde budou představeny ty, které se nejčastěji vyskytují [10, 17].

1. Phishing – Metoda, kdy je pomocí elektronické komunikace (e-mail, zprávy na sociálních sítích) rozeslán velký počet zpráv na různé adresy. Odeslané e-maily či zprávy se tváří jako klasické, které na první pohled nevypadají neškodně, zároveň často přijdou od adresáta, kterého příjemce zná. V e-mailu je odkaz, který po rozkliknutí přesměruje příjemce zprávy na podvodnou stránku. Kromě přesměrování na jinou stránku, lze touto cestou dostat do zařízení škodlivý vir. Tímto způsobem se útočník snaží z lidí získat citlivé údaje (např.: různá přístupová hesla, kódy či údaje od platebních karet). Phishingové e-maily lze rozeznat z chyb, které obsahují. Jedná se o gramatické chyby, překlepy v adrese atd. [23]. Nemusí se, ale jednat pouze o e-maily, mohou to být i podvodné hovory (vishing) nebo zasílání SMS zpráv (smishing). Útočník se může vydávat za pracovníka některé instituce, např.: banky či pojišťovny, a snaží se příjemce přesvědčit k rozkliknutí přijatého odkazu nebo zavolání na dané číslo. U těchto metod je často využívána taktika naléhavosti, což může být třeba zablokování bankovního účtu nebo nedoručení objednané zásilky [26]. Příklad takového smishingového útoku vyobrazuje obrázek 1. Metody

phishingu se neustále zlepšují a některé e-maily, ale i hovory je už těžší rozeznat, zda se opravdu jedná o podvod, či nikoliv. Nejspolehlivější ochranou před těmito útoky je ověřování přijatých zpráv. Všímat si, zda je adresát známý či neznámý, jak je e-mail či jiná zpráva napsána, zda se objevují stylistické či gramatické chyby [17].



Obrázek 1 – Příklad smishingového útoku (zdroj: vlastní)

2. Malware – Pojem malware se skládá ze slov software a malicious (neboli škodlivý). Je to tedy škodlivý software, který napadá a poškozuje systémy. Typů malware je několik, řadí se mezi ně např. spyware, adware, již zmíněný phishing či ransomware. Malware napadá zařízení, která nejsou dostatečně chráněna antivirovými programy. Do samotného systému se dostane skrz webové stránky, které jsou napadeny, skrze stažená data, přes různé soubory her a v neposlední řadě i e-mailem. Útočníci tímto způsobem získávají

osobní údaje, včetně hesel, nebo znemožňují přístup do zařízení. Ačkoliv napadení malwarem má své specifika, pro běžného uživatele počítače je těžko rozpoznatelný. Mezi tyto znaky se řadí např. zpomalení systému, zobrazování vyskakovacích oken, menší kapacita úložiště, ale i baterie. Nejúčinnější ochranou před tímto napadením je využívání různých antivirových programů, které zabraní škodlivému působení. I zde platí stejné pravidlo, jako u výše zmíněného phishingu, tedy neotvírat neznámé e-maily a přiložené odkazy. V neposlední řadě je důležité pravidelně zálohovat data [41, 42].

3. Ransomware – Je škodlivý software, který má za úkol zašifrovat a uzamknout data či celé počítače uživatelům a následně od nich vyžadovat výkupné pro odšifrování. Nejčastěji požadují zaplacení v bitcoinech či jiných kryptoměnách. Pokud se takto nestane útočník vše smaže a uživatel přijde o svá data. Ransomware se do počítače může dostat opět přes podvodné e-maily, nebo pokud se uživatel dostane na webové stránky, které jsou infikované. Typů ransomware je spousta, např.: Screen locker (uzamčení obrazovky), PIN locker (změna přístupového kódu) či nejčastěji využívaný kryptografický ransomware, který zašifruje data. Nejúčinnější ochranou před napadením je pravidelné zálohování dat a souborů či neotvírání podezřelých e-mailů a jejich odkazů a příloh. Tento způsob útoků se nejčastěji využíval během pandemie COVID-19 [10, 17, 24].

4. DDoS – Zkratka pochází z anglického názvu Distributed Denial of Service, do češtiny přeloženo jako „odepření služby“. Tento útok funguje na principu zasílání požadavků z více počítačů, které jsou infikované a jsou po celém světě (distribuovaná botnet síť). Při zahlcení velkého množství požadavků dojde k přetížení a následně ke

zpomalení výkonu napadené služby. V některých případech dojde k výpadku nebo úplnému přerušení fungování webové stránky či sítě. Často se tyto formy útoků využívají pro politicky motivované útoky či různé aktivisticky založené útoky. Kromě DDoS je ještě DoS (Denial of service), kde útok probíhá pouze z jednoho zařízení, ale princip je stejný jako u DDoS. Největším problémem těchto útoku je jejich eliminace, protože nestačí zničit jeden počítač, ale celou síť počítačů, který vedou tento útok [10, 25].

5. Man in the Middle – Častěji se využívá zkratka MITM. V tomto případě dochází k situaci, kdy se útočník začlení do konverzace mezi dvě zařízení, ve kterém vystupuje jako jedno ze zařízení a přijímá informace, které může dále využít k další činnosti [43]. Tím může získat osobní údaje či citlivé informace, které může následně využít pro svůj prospěch nebo jako prostředek k vydírání. Cracker také může získaná data či informace různě pozměňovat a upravovat. Nejčastěji k těmto útokům dochází skrze veřejné sítě Wi-Fi, nebo na webových stránkách, které nemají bezpečnostní certifikát. Tento útok je obzvlášť náročné rozpoznat, a proto se doporučuje využívat Wi-Fi sítě, které uživatel běžně používá a zná. V případě využití neznámé veřejné sítě je dobré se nikde nepřihlašovat [44].

3.2.6 Kybernetická bezpečnostní událost

Dle ZKB se kybernetickou bezpečnostní událostí rozumí: „*událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací*“ [2, § 7 odst. 1].

3.2.7 Kybernetický bezpečnostní incident

Druhý pojem, který ZKB definuje je kybernetický bezpečnostní incident, kterým se rozumí: „*narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události*“ [2, § 7 odst. 2].

Oproti kybernetickému útoku je rozdíl v kybernetickém bezpečnostním incidentu v jeho zavinění. Jak již bylo výše zmíněno kybernetický útok je čistě úmyslný čin na rozdíl od incidentu, který může být způsoben jak úmyslně, tak i nedbalostně. Jako kybernetický bezpečnostní incident se považuje i působení tzv. „vyšší moci“. Vyšší moc, pojem pochází z latinského vis maior, a v tomto případě znamená nějakou událost nebo okolnost, která nastala a nešlo se ji vyhnout nebo nějak předejít [11]. Příkladem takové vyšší moci může být válka či přírodní katastrofy, což může být zemětřesení nebo povodeň [9].

3.2.8 Kybernetická bezpečnost

Kybernetická bezpečnost je často chápána odlišně. V různých odborných publikacích se tento pojem vyskytuje pod různými definicemi. Např. Výkladový slovník kybernetické bezpečnosti ji definuje jako: „*souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru*“ [8, s. 97].

Hlavním úkolem celkové bezpečnosti je ochrana dané věci či objektu před nežádoucími vlivy, jejím poškozením či zničením [17]. U KB se pouze vše přenáší do kybernetického prostoru a vše s ním související. KB v sobě zahrnuje bezpečnost kybernetického prostoru, ochranu počítačového a informačního systému před napadením či ochranu samostatných uživatelů v kybernetickém prostoru. Proto jako nejvhodnější definice KB lze uvést: „*souhrn právních, organizačních, technických a vzdělávacích prostředků, které směřují k zajištění*

ochrany počítačových systémů a dalších prvků ICT, aplikací, dat a uživatelů, schopnost počítačových systémů a využívaných služeb reagovat na kybernetické hrozby či útoky a jejich následky, jakož i plánování obnovy funkčnosti počítačových systémů“ [9, s. 44-45]. V KB se používá označení CIA pro označení tři nejdůležitější oblastí, které je potřeba chránit. Tyto oblasti jsou:

- confidentiality (důvěrnost)
- integrity (integrita)
- availability (dostupnost).

3.2.9 Kybernetický prostor

Prostor, kde KÚ probíhají, se nazývá kybernetický prostor. Zkráceně se častěji využívá výraz kyberprostor a vychází z anglického překladu slova cyberspace [1]. Tento pojem bývá často velmi diskutovaný z důvodu různých až často rozdílných definic. Dosud nebyla stanovena žádná jednotná definice na mezinárodní úrovni, která by ho jasně definovala [15]. Tento termín je relativně mladý, protože úplně poprvé byl použit v roce 1982, kanadským spisovatelem Williamem Gibsonem. Postupem času pojem začali využívat i jiní autoři ve svých pracích. John Perry Barlow byl první, kdo charakterizoval kybernetický prostor v souvislosti s počítačovými sítěmi. Podle Sofie Tzimopoulové je kyberprostor vnímán jako imaginární místo, kde je možné vystupovat za jinou identitu, kterou si člověk zde vytvoří než v reálném světě. I v současné době se tento pojem interpretuje různě [12, 15].

Například ZKB definuje kybernetický prostor jako „*digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.*“ [2, §2 odst. 1, písm. a]

Trochu rozdílná definice se objevuje v knize Kybernetická bezpečnost II, kde je kyberprostor charakterizován jako: „*virtuální svět vytvořený moderními*

technologickými prostředky, v němž se informace vytvářejí, zpracovávají, ukládají a šíří pomocí elektromagnetického vlnění.“ [12, s. 10]

Ačkoliv je mezi oběma těmito definicemi nepatrný rozdíl, obě se shodují, že kybernetický prostor je nějaký svět, který je nefyzickým místem, ačkoliv se v něm pohybují lidé. Je tvořen navzájem propojenými sítěmi počítačů, ale také třeba cloudovými úložišti [9, 12]. To tedy znamená, že bez reálného světa by virtuální svět nemohl fungovat a ani existovat [9]. Kromě toho, že tento prostor nemá pořádně ustálenou definici, nemá dané ani svoje hranice a rozměr. Co se týče rozměru ten je neurčený, nemá konec ani začátek. Nemá žádné striktně dané ohraničení. Problémem neurčených hranic je, že dochází k přelévání kyberkriminality mezi státy a vzniká tak nespočet právních problémů. Nebo také může docházek ke kybernetickým válkám, protože spousta státu chápe kyberprostor jako novou válečnou zónu [1]. Účastníkem KP v dnešní době jsou skoro všichni [12].

3.2.10 Kybernetická kriminalita

Známá také pod názvem jako počítačová kriminalita nebo častěji využívaný zkrácený pojem kyberkriminalita. Kybernetickou kriminalitu lze chápat jako trestnou činnost páchanou v kybernetickém prostoru pomocí informačních a komunikačních technologií nebo počítačů. Kromě trestné činnosti páchané pomocí počítačů sem patří také činnost zaměřená proti nim [20].

V ČR každoročně stoupá případů týkající se kybernetické kriminality. Nejvíce se nárůst projevil během pandemie COVID-19, kdy značná část lidí musela pracovat z domu s využitím počítačů. Největší zastoupení měly podvody, z větší části mezi soukromými osobami, dále to byly neoprávněné přístupy do cizích zařízení. Stejně časté byly i úvěrové podvody a hacking. V pomyslném žebříčku páchané kriminality své místo mají i různé druhy podvodů (tzv. phishing) [21].

Ke snížení kriminality ve státě a v boji proti ní je vydána ministerstvem vnitra „Strategie prevence kriminality v České republice na léta 2022 až 2027“, ve které je i kapitola věnovaná kybernetické kriminalitě. Jsou zde podrobněji rozepsány cíle, které by měly být splněny během působení této strategie. Např. více se zaměřit na děti, které se pohybují v KP, rozšíření mezi uživatele informačních technologií, lepší znalost a poučení ohledně správného a bezpečného fungování s informačními technologiemi a na internetu či vybudování poradenského systému pro pomoc při řešení či pro samotné oběti této kriminality [22].

3.2.11 Kybernetický terorismus

„*Trestná činnost páchaná za primárního využití či cílení prostředků IT s cílem vyvolat strach či neadekvátní reakci. Používá se nejčastěji v kontextu extremisticky, nacionalisticky a politicky motivovaných útoků*“ [8, s. 101].

Do současné doby se ještě neodehrál KÚ, který by byl považován jako kybernetický terorismus. Klasické teroristické útoky si vyžádají mnoho obětí, což se v případě KÚ zatím nestalo. Takže se zatím jedná o pojem, který je možno nalézt v několika publikacích, ačkoliv není možné tento pojem přisoudit některému z již provedených útoků. S největší pravděpodobností se ale tento pojem může časem stát reálný [45].

3.2.12 Kybernetická válka

„*Použití počítačů a internetu k vedení války v kybernetickém prostoru. Soubor rozsáhlých, často politicky či strategicky motivovaných, souvisejících a vzájemně vyvolaných organizovaných kybernetických útoků a protiútoků*“ [8, s. 99].

Válka tedy nemusí probíhat jen na zemi, ve vzduchu či na vodě, ale i v KP. V roce 2016 byl KP uznán jako válečnou doménou [1].

3.2.13 Kybernetická obrana

„Obrana proti kybernetickému útoku a zmírnění jeho následků. Nebo rezistence subjektu na útok a schopnost se účinně bránit“ [1, s. 13].

Proti KÚ je důležité se taky bránit, aby nedocházelo k větším škodám a zmírnit následky provedeného útoku.

3.2.14 Kybernetická strategie

„Obecný postup k rozvoji a využití schopností pracovat v kybernetickém prostoru, integrovaný a koordinovaný s ostatními operačními oblastmi k dosažení nebo podpoře dosažení stanovených cílů pomocí identifikovaných prostředků, metod a nástrojů v určitém časovém rozvrhu“ [1, s. 13].

3.3 Kritická informační infrastruktura

Definici KI vymezuje zákon č. 240/2000 Sb., Zákon o krizovém řízení a o změně některých zákonů neboli krizový zákon jako: *„kritickou infrastrukturou prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení, jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu“* [40, § 2, písm. g].

KII je podmnožina KI, kterou pak definuje ZKB jako: *„kritickou informační infrastrukturou prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti“* [2, § 2 odst. 1 písm. b].

3.4 Specifika kybernetického ohrožení zdravotnického zařízení

V případech kybernetického ohrožení zdravotnických zařízení lze vysledovat určité společné znaky, jako např. typ útoku a jeho motivaci, šíře dopadu a časová tíseň při jeho řešení. Zdravotnické zařízení je zařízení, jehož úkolem je

poskytování zdravotní péče. Z toho plynou určitá specifika či zvláštní rizika, pokud čelí takové zařízení hackerskému útoku. Z povahy zařízení je zřejmé, že pracuje s velkým množstvím dat, a to jednak s osobními údaji pacientů, ale také s dalšími daty souvisejícími s poskytováním zdravotní péče, jako např. anamnézou pacienta, historií zdravotní péče a plánem pro následující zdravotní péči. Tyto znaky přivádí k jednomu ze specifických bodů kybernetického ohrožení, konkrétně k jeho motivaci. Tou může být u zdravotnických zařízení jednak snaha získání osobních údajů, neveřejných výsledků výzkumu tak i znemožnění poskytnutí zdravotního ošetření či jiných úkonů.

Dalším specifikem je pak šíře dopadů hackerského útoku na zdravotnické zařízení. Na rozdíl od útoků vedených na soukromé společnosti jiných odvětví může útok v prostředí zdravotnického zařízení znemožnit poskytnutí zdravotní péče, čímž může zasáhnout také část civilního obyvatelstva. Konkrétním příkladem takto širokého dopadu může být např. KÚ vedený na Nemocnici Rudolfa a Stefanie v Benešově, jehož detaily uvádí tato práce v následující kapitole.

S ohledem na specifika je dalším společným znakem útočníka nebo skupiny útočníků využít časové tísně k získání finanční odměny za ukončení útoku nebo opětovné zprovoznění komunikačních a informačních systémů a ostatních podporovaných služeb v daném zdravotnickém zařízení.

Při uvážení všech výše zmíněných společných znaků lze odvodit, že specifickým a nejčastějším útokem na zdravotnické zařízení je ransomwarový útok. Dojde-li v prostředí zdravotnického zařízení k tomuto typu útoku a dojde k zašifrování nebo znepřístupnění dat na pevných a síťových discích, není možné pracovat s údaji a daty pacientů, data nemohou být sdílená prostřednictvím komunikačních systémů a nemůže být poskytnuta zdravotní péče. Jedná-li se

o neodkladnou zdravotní péči, splňuje útok i specifický znak časové tísně, kdy útočník doufá v zaplacení výkupného [28, 39].

3.5 Kybernetické útoky na nemocniční zařízení v ČR

V ČR došlo během několika let ke KÚ, které byly zaměřeny na nemocniční a obdobná zařízení. Níže budou popsány dva největší a nejmedializovanější proběhlé útoky na nemocniční zařízení v ČR.

3.5.1 Nemocnice Rudolfa a Stefanie v Benešově

Útok se stal ve středu 11. prosince 2019, kdy nemocnice byla napadena počítačovým virem, ransomware Ryuk. Útočník zašifroval data v počítačích a vyžadoval výkupné. V den útoku nemocnice fungovala v omezeném režimu, nebylo možné spustit žádné počítače, ani žádné jiné laboratorní či zdravotnické přístroje, kvůli čemuž musely být plánované operace zrušeny. Část pacientů musela být převezena do okolních nemocnic. Největší ztráty zaznamenala nemocnice v souvislosti s omezením lékařských výkonů, dále to byly neproplacené finanční částky od zdravotních pojišťoven za plánované operace a zákroky. Nemalé peníze nemocnice vložila do nového zabezpečovacího systému a do práce na obnově poškozených softwarů. Celková odhadovaná škoda se vyšplhala na 59 milionů Kč. Do plného provozu se nemocnice vrátila až 30. prosince 2019 [27, 28]. Celý tento útok začal phishingovým e-mailem s odkazem, který otevřel někdo ze zdravotnického personálu, čímž došlo k instalaci jiných nebezpečných kmenů malware [28].

3.5.2 Fakultní nemocnice v Brně

Obdobně jako benešovská nemocnice se Fakultní nemocnice („dále jen FN“) v Brně stala 13. března 2020 terčem KÚ. Kromě samotné nemocnice byla postižena i Dětská nemocnice společně s porodnicí sídlící mimo areál fakultní nemocnice. Jako u předchozího útoku se jednalo o ransomware útok. Na začátku

celého útoku opět došlo, jako u předchozího případu, k otevření phishingového emailu, který vypadal jako e-mail od někoho známého. Tím se virus dostal do počítače, čímž začal zašifrovávat data. Postupně začalo docházet ke zpomalování počítačů a systémů, až došlo k výpadku. Ačkoliv nedošlo vlivem útoku k vypnutí všech počítačů, z důvodu bezpečnosti byly vypnuty všechny. Péče v nemocnici musela být omezena, plánované operace a zákroky musely být zrušeny a akutní pacienti byli převáženi do jiných nemocnic [29]. Nikdo při útoku nebyl ohrožen na životě a pouze zde došlo k finanční škodě a ztrátě některých údajů informačního systému používaného pro řízení procesů v nemocnici. Zde se finanční škoda dostala na 150 milionů korun. Pachatel tohoto útoku nebyl nikdy dohledán [30].

Kromě těchto dvou zmíněných KÚ došlo v ČR k dalším několika desítkám podobných situací, kdy nemocnice musely čelit takovým útokům. Dalšími příklady mohou být uvedeny útok v roce 2018 na nemocnici v Janově na Rokycansku, v roce 2020 na Psychiatrickou nemocnici Kosmonosy. Ve stejném roce se stala terčem KÚ FN Olomouc, pardubická či ostravská nemocnice. O rok později v Praze byly KÚ napadeny tři polikliniky. V roce 2022 to pak byla Krajská nemocnice v České Lípě [31].

3.6 Kybernetické útoky na nemocniční zařízení v zahraničí

I ve světě musí nemocnice čelit KÚ stejně jako v ČR. V následujících podkapitole bude popsán nejznámější provedený KÚ na nemocniční zařízení.

3.6.1 Fakultní nemocnice Düsseldorf

Incident se stal 10.9.2020, kdy se terčem útoku stala FN Düsseldorf. Útočník využil slabých míst v softwaru, VPN (virtuální privátní síť), čímž došlo k selhání informačních systémů v nemocnici. I v tomto případě se jednalo o ransomware útok. Ten se týkal urgentního příjmu [47]. Po útoku nemocnice musela fungovat

v omezeném režimu. Kromě finanční ztráty sebou tento útok nesl i tragický následek, úmrtí pacientky. Vlivem nefunkčnosti systémů v Düsseldorfské nemocnici, které pacientka nutně potřebovala, musela být převezena do jiné nemocnice, přibližně vzdálené 30 km, čím se léčba opozdila o skoro hodinu. Jedná se o první případ KÚ, při kterém přišel o život člověk [32, 33, 47]. Z dostupných zdrojů se nemělo jednat o útok na nemocnici, ale nýbrž na místní univerzitu. Poté co se útočníci dozvěděli, že útok je veden na nemocnici předali šifrovací klíč policii [47]. S největší pravděpodobností tento krok ze strany útočníků pomohl k zamezení větších ztrát. Úplný provoz nemocnice byl obnoven po dvou týdnech [32, 33].

4 METODIKA

Tato část bude obsahovat popis zvolených metod, které byly použity pro zpracování praktické části této práce. Zvolenými metodami jsou metoda strukturovaného individuálního rozhovoru s odborníky na danou problematiku použitá pro získaní dat a informací a metoda interpretativní fenomenologické analýza (dále jen „IPA“), kterou byla následně data získaná z rozhovorů vyhodnocena.

Strukturovaný neboli standardizovaný rozhovor je jednou z metod kvalitativního výzkumu, kterým se získávají data zejména v sociologickém výzkumu. Ve strukturovaném rozhovoru jsou pokládány předem připravené otázky v přesně stanoveném pořadí. Tazatel se dále neptá na žádné doplňující otázky a ani nijak nereaguje na vývoj rozhovoru doplněním otázek z dalších souvisejících oblastí [47].

Metoda interpretativní fenomenologické analýzy je založena na principu porozumění zkušenosti člověka, který se v dané problematice pohybuje a pomáhá tak prozkoumat význam zkušeností pro dotazovaného člověka, čímž napomáhá porozumět jednotlivým informacím (fenoménu), které respondent předává [55].

Rozhovoru se zúčastnili 4 respondenti, kteří byli vybráni vedoucím práce. Z důvodu velkého časového vytížení respondentů proběhly dva rozhovory distančně, formou e-mailové komunikace, zbylé dva rozhovory proběhly během osobního setkání s daným respondentem. Z důvodů bezpečnosti a ochrany citlivých informací však respondenti neudělili souhlas s nahráním rozhovoru. Tabulky se zaznamenanými odpověďmi uvedené v následující kapitole, tak obsahují doslovný přepis textů obdržených od respondenta č. 1 a č. 2, a doslovný zápis odpovědí u respondenta č. 4. Respondent č. 3 si pak nepřál ani doslovný

zápis svých odpovědí, a tak jsou v tabulce uvedeny pouze informace vyplývající z respondentových odpovědí, které následně sám respondent zkontroloval a schválil.

Rozhovor byl složen z dvanácti otázek, na které respondenti postupně odpovídali. Odpovědi respondentů byly zaznamenány do jednotlivých tabulek, kdy každé ke každé otázce byla vytvořena jedna tabulka a odpovědi respondentů byli zapisovány do připravených polí. Jednotlivé tabulky pak byly slovně vyhodnoceny. Celý rozhovor byl pak rozdělen do dílčích témat vyhodnocen metodou IPA.

5 VÝSLEDKY

V této kapitole jsou uvedena data mapující současný stav na poli problematiky ochrany zdravotnických zařízení před kybernetickými útoky. Data byla získávaná formou strukturovaných rozhovorů s osobami, které se v rámci zdravotnického zařízení podílejí na správě informační a komunikační sítě a zajištění kybernetické bezpečnosti. Takto získaná data byla následně vyhodnocována pomocí metody interpretativní fenomenologické analýzy.

Z důvodů zachování bezpečnosti a ochrany citlivých informací jsou odpovědi uváděny pouze v obecné rovině. Z tohoto důvodu byli dále jednotliví respondenti anonymizování, přičemž v práci jsou uvedeny pouze údaje o zařazení a funkci jednotlivých respondentů. Získaná data jsou taktéž anonymizována a neobsahují informace kterého zdravotnického zařízení se jednotlivé odpovědi konkrétně týkají. Pro potřeby práce je tento přístup zcela dostačující, jelikož hlavním cílem je mapování obecného současného stavu na poli ochrany zdravotnických zařízení před kybernetickými útoky v rámci ČR, a nikoliv analýza zabezpečení konkrétní nemocnice.

Data jsou uváděna v jednotlivých tabulkách, přičemž každá tabulka se týká jedné otázky, ke které jsou přiřazeny odpovědi jednotlivých respondentů. Pod tabulkou následuje vždy text obsahující vyhodnocení odpovědí respondentů a zdali se ve svých odpovědích shodují, či mají odlišný pohled na dotazovanou problematiku. Tato část také obsahuje tabulku, kde je k jednotlivým respondentům uvedeno jejich zařazení a funkce v rámci zdravotnického zařízení, kde pracují.

Tabulka 1 - Funkce respondentů (zdroj: vlastní)

Respondent	**Funkce ve zdravotnickém zařízení**
1	specialista oddělení bezpečnostní a provozní správy IS
2	specialista oddělení vnitřního řízení
3	manažer kybernetické bezpečnosti
4	specialista kybernetické bezpečnosti

5.1 Data získaná z rozhovorů a vyhodnocení jednotlivých otázek

Tabulka 2 – Odpovědi k otázce č. 1 (zdroj: vlastní)

Otázka č. 1	
Jaká opatření a nástroje používáte pro zajištění kybernetické bezpečnosti v nemocnici?	
Odpovědi	
Respondent č. 1	*„Mezi hlavní nástroje ochrany pracovních stanic zaměstnanců naší organizace patří antivirový program, nástroj pro monitoring síťových prvků včetně stanic a serverů, zabezpečená VPN pomocí dvoufázové autentizace a nástroj pro vyhodnocování logů.“*
Respondent č. 2	*„Lze hovořit o dvou cestách k zajištění kybernetické bezpečnosti, které jsou na sobě závislé.“* *„První cestou jsou organizační opatření, která vycházejí ze zákona o kybernetické bezpečnosti, vyjmenuji některé:* *1) zvyšování povědomí svých zaměstnanců o problematice kybernetické bezpečnosti (edukace);* *2) tvorba a aktualizace analýzy rizik v dané oblasti;* *3) řízení definovaných rizik z vypracované analýzy;* *4) pravidelné audity;* *5) evidence významných dodavatelů;* *6) řízení přístupu osob;* *7) řízení aktiv;* *8) řešení kybernetických bezpečnostních událostí a incidentů.“* *„Druhou cestou jsou technická opatření. V rámci bezpečnosti bohužel nemohu být k technickým opatřením konkrétní, nicméně standardem může být například používání níže uvedených nástrojů:* *1) Endpoint security (antivir na koncových stanicích);* *2) SIEM (Security information and event manager)* *3) Firewall;* *4) Spamfilter.“*

Respondent č. 3	Technická a organizační opatření. Mezi technická se řadí firewall, antivirus, antispam, monitoring, sběr a vyhodnocení logů. Organizační opatření jsou různé předpisy a školení, bezpečnostní tým, varování.
Respondent č. 4	*„EDR (Endpoint Detection and Response) – pomáhá nám k ochraně koncových prvků, před škodlivými viry."* *„SIEM (Security Information and Event Management), to je zabezpečení, které pomáhá detekovat hrozby a analyzovat je."* *„Dále jsou to různé antispamové a antivirové programy."*

Otázka č. 1 se věnuje opatřením a nástrojům využívané v nemocnici pro zajištění KB. Dotázaní respondenti se shodují na technických a organizačních opatření. Z uvedených technických opatření se nejčastěji využívá firewall a různé druhy antivirových programů. Dále je to EDR či SIEM. Z bezpečnostně-provozních důvodů nemohou být uváděny podrobnosti a konkrétní způsoby zabezpečení, viz. respondent č.2.

Tabulka 3 - Odpovědi k otázce č. 2 (zdroj: vlastní)

Otázka č. 2	
Kolik osob má ve Vaší nemocnici na starost zabezpečení KB?	
Odpovědi	
Respondent č. 1	*„V našem týmu je pouze manažer kybernetické bezpečnosti a datový specialista, takže 1,5 člověka."*
Respondent č. 2	*„Oddělení kybernetické bezpečnosti se skládá z několika osob, zároveň spolupracujeme s Odborem informatiky a externími odborníky v dané problematice."*
Respondent č. 3	Řídící orgán pro KB, Výbor pro řízení KB, oddělení KB. Dále IT, právní oddělení. Na KB se podílí i ostatní zaměstnanci svým chováním.
Respondent č. 4	*„Je to 4–5 osob, včetně IT oddělení"*

Tato otázka se týká personálního zabezpečení KB. Největší roli hraje oddělení kybernetické bezpečnosti. Následně je to oddělení IT. Respondent č. 3 uvádí, že kromě všech odborně způsobilých zaměstnanců, kteří se starají o bezpečnost se na KB podílí všichni zaměstnanci nemocnice svým chováním. Respondent č. 4 odpovídá, že o kybernetickou bezpečnost se v nemocnici stará 4–5 lidí, včetně IT specialistů.

Tabulka 4 - Odpovědi k otázce č. 3 (zdroj: vlastní)

Otázka č. 3	
Jak vnímá kybernetické hrozby a z nich plynoucí rizika management Vaší nemocnice?	
Odpovědi	
Respondent č. 1	*„Pokud by nebylo útoků na jiné nemocnice, tak by kyberbezpečnost byla vždy až na posledním místě. Nyní se doba změnila a vedení tuto problematiku zavnímalo.“*
Respondent č. 2	*„Žijeme v době, kdy se spousta druhů kriminality přesouvá do kyberprostoru. Snažíme se naše vedení maximálně informovat a edukovat v dané problematice“* *„Náš management si problematiku kybernetické bezpečnosti uvědomuje, a proto bere každou kybernetickou hrozbu velmi vážně.“*
Respondent č. 3	V tomto ohledu vedení plně podporuje jakékoliv opatření proti kybernetickým útokům.
Respondent č. 4	*„Nedostatečně. Více by se chtělo se zaměřit na školení a větší informovanost o zranitelnosti informačních a komunikačních technologií.“*

Z odpovědí na otázku č. 3 vyplývá, že managmenty nemocnic tuto problematiku většinou vnímají, výjimka je u odpovědi respondenta č. 4, který uvádí, že managment problematiku kybernetických útoků vnímají nedostatečně. Respondent č. 1 dodává, že pokud by se dříve nestaly žádné KÚ, bohužel by se tato problematika tolik neřešila. Podle respondenta č. 2 bere managment nemocnice každou kybernetickou hrozbu velmi vážně.

Tabulka 5 - Odpovědi k otázce č. 4 (zdroj: vlastní)

Otázka č. 4	
Jak zabezpečujete vzdělání zaměstnanců a personálu a jak často v oblasti kybernetické bezpečnosti?	
Odpovědi	
Respondent č. 1	*„Každý nový zaměstnanec prochází vstupním školením, kde je mimo jiné také zařazena přednáška a online kurz. Zaměstnanci IT povinně absolvovali školení „dávej Kyber" od NUKIBu. Manažer kybernetické bezpečnosti navštěvuje porady Vrchních sester, kde touto cestou předává informace o aktuálním dění ve světě online, prostředí intranetu."*
Respondent č. 2	*„Každý nastupující zaměstnanec musí podstoupit školení v oblasti kybernetické bezpečnosti, kde je seznámen s možnými hrozbami, se kterými se lze setkat. Zaměstnancům jsou demonstrovány některé hrozby a jsou informování o tom, jak na ně reagovat."* *„Zároveň je zaměstnanec seznámen se základními pravidly k zachování bezpečnosti jednotlivce, jelikož zodpovědný a opatrný jedinec je klíčový pro zachování bezpečnosti celé organizace."* *„Mimo nástupní školení se naši zaměstnanci vzdělávají v dané oblasti prostřednictvím e-learningového kurzu, který je vytvořen naším manažerem kybernetické bezpečnosti. E-learningový kurz obsahuje veškeré potřebné doporučení pro zodpovědné chování jedince při práci s informační komunikační technologií jako takovou, na internetu i mimo něj."* *„Mimo veškerá školení jsou naši zaměstnanci informováni o aktuálních hrozbách z kyberprostoru každý týden v článku vypracovávaným naším manažerem kybernetické bezpečnosti."*
Respondent č. 3	Nástupním školení musí projít každý nový zaměstnanec. Skládá se z úvodní prezentace, následně školení na Moodlu a na závěr zaměstnanec musí složit test (forma edukační). Toto školení se musí každoročně zopakovat. Kromě tohoto školení jsou zaměstnancům průběžně zasílány různá varování a články cestou intranetu do tzv. „Kyber okénka".

Respondent č. 4	*„Formou školení v rámci bezpečnosti a ochrany zdraví při práci 2x ročně, nebo samostatným školením v kybernetické bezpečnosti, pokud se něco stane. Ale i tak je to, dle mého názoru, nedostatek školení v této oblasti.“*

Otázka č. 4 se zaměřuje na vzdělávání zaměstnanců a personálu nemocnice. Z odpovědí je patrné, že nemocnice klade velký důraz na školení a vzdělávání v rámci KB. Respondenti se shodují, že každý nový zaměstnanec musí projít vstupním školením, které se skládá z přednášky a online školení. Tento kurz by měl nově nastupujícím zaměstnancům předat informace, jak předcházet hrozbám, a popřípadě jak na vzniklé situace reagovat. Kromě samotného školení na zacházení s informačními a komunikačními zařízeními je kladen důraz na fungování jedince na internetu. Respondent č. 1 ještě otázku doplňuje tím, že zaměstnanci IT musí projít kurzem vytvořeným NÚKIBem. Z odpovědí lze vyčíst, že významnou roli v KB má manažer kybernetické bezpečnosti. Ten předává informace vrchním sestrám o novinkách, které se dějí v kybernetickém světě a mohly by jakkoliv narušit chod oddělení. Kromě toho vytváří online kurzy a píše články do „Kyber okénka“. Respondent č. 4 doplňuje školení v bezpečnosti a ochraně zdraví při práci.

Tabulka 6 - Odpovědi k otázce č. 5 (zdroj: vlastní)

Otázka č. 5	
Jaké konkrétní opatření používáte v souvislosti s obranou proti phishingu?	
Odpovědi	
Respondent č. 1	*„Jako nejúčinnější nástroj proti phishingu, phishingovým kampaním se nám potvrdilo: Varování prostřednictvím intranetu v „Kyber okénku" a neustálá edukace personálu."*
Respondent č. 2	*„Klíčovým opatřením je správná a pravidelná edukace zaměstnanců o problematice Phishingu a Spearphisingu. Každý zaměstnanec by měl mít v paměti, že existuje něco jako Phishing a měl by být schopen ho na základě školení identifikovat. V případě obdržení podezřelého e-mailu by zaměstnanec neměl otevírat žádné odkazy ani stahovat a otevírat přílohy, naopak by měl o této skutečnosti informovat Oddělení kybernetické bezpečnosti."* *„Technickým standardem je např. používání kvalitního spamfilteru, firewallu atd."*
Respondent č. 3	Proti phishingu jako technické opatření je využíván Firewall a antivirové programy. Avšak důležitější je lidský firewall, tedy poučený a vyškolený uživatel.
Respondent č. 4	*„Filtraci (blacklist a whitelist), školení personálu a antivirové programy."*

Z otázky č. 5 vyplývá, že nejúčinnější ochranou před phishingem, na které se respondenti jednoznačně shodli, je kvalitně proškolený zaměstnanec, který dokáže rozpoznat phishingový e-mail. Respondenti č. 2 a 3 ještě svými odpověďmi doplňují použití firewallu.

Tabulka 7 – Odpovědi k otázce č. 6 (zdroj: vlastní)

Otázka č. 6	
Jaké konkrétní opatření používáte v souvislosti s obranou proti ransomware?	
Odpovědi	
Respondent č. 1	*„Zakázali jsme spouštění a instalaci aplikací uživatelům.“*
Respondent č. 2	*„Standardem je např.: provádění pravidelných záloh, používání kvalitního spamfilteru, Firewall, dodržování fyzické bezpečnosti, edukace zaměstnanců.“*
Respondent č. 3	Technická opatření jako u phishingu a edukace personálu.
Respondent č. 4	*„Opatřením je provádění záloh ve formátu 3-2-1, to znamená 3 zálohy na dvou různých zařízení a jedna kopie mimo nemocnici, dále DRP a neotvírat neznámé přílohy.“*

Tabulka 6 zahrnuje odpovědi týkající se otázky zabezpečení proti ransomware. Odpovědi na tuto otázku jsou velmi podobné otázce č. 5, tedy edukace personálu, firewall a jiné antivirové programy. Jediný respondent č. 1 uvádí, že v nemocnici je zakázáno stahovat jakékoliv aplikace do počítačů. Poslední respondent uvádí, že důležité jsou zálohy v režimu 3-2-1, což respondent i sám vysvětlil.

Tabulka 8 - Odpovědi k otázce č. 7 (zdroj: vlastní)

Otázka č. 7	
Jaké změny byly ve vaší nemocnici provedeny po kybernetických útocích na nemocnici v Benešově a na FN v Brně?	
Odpovědi	
Respondent č. 1	*„Toto je velmi důležitý moment pro kyberbezpečnost obecně, protože do událostí v Benešově atd. došlo k zavnímání problematiky a dopadů takového útoku i mezi vedení a ostatní zaměstnance. V našich silách bylo upravit školení – „povědomí o informační bezpečnosti“*
Respondent č. 2	*„V rámci zajištění maximální možné dostupnosti, integrity a důvěrnosti dat byla provedena opatření na základě doporučení NÚKIB. Více konkrétní být bohužel nemohu.“*
Respondent č. 3	Opatření v době útoků už nemocnice měla nastavené. Uposlechnutí varování od NÚKIBu, které vydal v reakci na tyto útoky.
Respondent č. 4	*„Byla to spíše panika. Reálné změny spíše žádné.“*

Otázka č. 7 s zabývala změnami po útocích na nemocnici v Benešově a na FN v Brně. Tyto útoky hrály klíčovou roli ke zlepšení KB v nemocnicích, což potvrzuje svojí odpovědí respondent č. 1. Pro zachování bezpečnosti nemocnice není možné říci konkrétní opatření (viz respondent č. 2). Nemocnice proto provedla opatření, které vydal NÚKIB. Avšak rozdílnou odpověď uvedl respondent č. 4, že k žádným změnám nedošlo.

Tabulka 9 - Odpovědi k otázce č. 8 (zdroj: vlastní)

Otázka č. 8	
Jaké jsou podle Vás největší limity v oblasti kybernetické bezpečnosti nemocnice?	
Odpovědi	
Respondent č. 1	*„Personální zabezpečení a podfinancování.“*
Respondent č. 2	*„Jako největší limit pro dosažení maximální možné kybernetické bezpečnosti vnímám nedostatečné množství odborníků v dané oblasti na trhu.“*
Respondent č. 3	Mezi největší limity patří nedostatek financí na zabezpečení kybernetické bezpečnost a nedostatek lidí.
Respondent č. 4	*„Implementování bezpečnosti do systémů, který nebyli vybudovány s ohledem na bezpečnost. Druhou věcí je nedostatek lidských zdrojů.“*

V otázce č. 8, která se zabývá limity zabezpečení KB nemocnic, se respondenti shodují ve stejných odpovědích, a tou je personální nedostatek. Respondent č. 2 uvádí nedostatečné financování kybernetické bezpečnosti. Poslední respondent si myslí, že největší limit je v implementování bezpečnosti do systémů, které jsou vybudovány pro jiné účely než bezpečnost.

Tabulka 10 - Odpovědi k otázce č. 9 (zdroj: vlastní)

Otázka č. 9	
Jakými konkrétními kroky vnímáte podporu Ministerstva zdravotnictví a jiných vládních úřadů v posílení kybernetické bezpečnosti nemocnice?	
Odpovědi	
Respondent č. 1	*„Pokud se bavíme o naší organizaci, tak naším zřizovatelem není Ministerstvo zdravotnictví... takže bych se vyjádřil pouze k NÚKIBu, který u nás prováděl bezpečnostní audit a na základě výsledků tohoto auditu jsme přijali opatření.“*
Respondent č. 2	*„Subjektivně je vnímám pozitivně, nicméně naším zřizovatelem není Ministerstvo zdravotnictví. Tudíž si nejsem jist, zdali se nás podpora ze strany Ministerstva zdravotnictví jakkoli dotýká.“*
Respondent č. 3	Největší podpora přichází od resortního ministerstva a NÚKIBu.
Respondent č. 4	*„Absolutně žádné. Ministerstvo zdravotnictví rezignovalo v oblasti kybernetické bezpečnosti.“*

Otázka č. 9 se týkala podpory ze strany Ministerstva zdravotnictví. Tato otázka byla bohužel špatně formulována, jelikož tři respondenti byli ze zdravotnického zařízení, které je zřízeno jiným ministerstvem, než je ministerstvo zdravotnictví. Respondent č. 1 se tak vyjádřil pouze ke spolupráci s NÚKIBem, respondent č. 2 odpověděl, že podporu ze strany ministerstva zdravotnictví vnímá pozitivně, ale vzhledem k tomu, že jeho organizace taktéž, jako v případě respondenta č. 1, není zřizovaná Ministerstvem zdravotnictví, vyjádřil pochybu, zda se jejich organizace podpora týká. Respondent č. 3 pak řekl, že jejich zařízení přihází podpora ze strany resortního ministerstva. Respondent č. 4 pak uvedl, že Ministerstvo zdravotnictví v této oblasti rezignovalo, a tak žádnou podporu nevnímá.

Tabulka 11 - Odpovědi k otázce č. 10 (zdroj: vlastní)

Otázka č. 10	
Myslíte si, že je kybernetická bezpečnost dostatečně financována? Pomohlo by navýšení financí k lepšímu zabezpečení informačních systémů před kybernetickými útoky?	
Odpovědi	
Respondent č. 1	*„Kyberbezpečnost je obecně podfinancována, totéž platí o IT. Většinou si vedení neuvědomí, že když se vybuduje složitá infrastruktura, tak že je potřeba udržovat „krok". Na následnou obměnu, či upgrade se už peníze nenajdou."*
Respondent č. 2	*„Myslím si, že by jistě bylo vhodné financovat více. Je zde ovšem nutno podotknout, že se situace vyvíjí dobrým směrem. Organizace si již uvědomují nebezpečí hrozící z kyberprostoru a snaží se reagovat. Spoustu firem nyní investuje nemalé částky k zajištění maximální možné bezpečnosti. Jako problém ovšem vnímám nedostatek odborníků v daném odvětví."*
Respondent č. 3	Nikdy nebude dostatek financí na zabezpečení kybernetické bezpečnosti.
Respondent č. 4	*„Ano, pokud se jedná o investiční peníze. Za tyhle peníze se dá koupit spousta vylepšených systémů k zabezpečení, nových hardwarů a softwarů a podobně. Ale zároveň ne, protože nelze koupit lidi. Protože je potřeba mít lidi, kteří s tím umí. Navýšení financí by pomohlo, ale v neinvestiční složce. Tedy více zainvestování do personálu."*

Otázka č. 10 se zabývá financováním bezpečnosti. Všichni respondenti se shodují na nedostatečném financování KB. Jediný respondent č. 4 uvádí, že je investován dostatek peněz do nákupu nových systémů k lepšímu zabezpečení. Respondent č. 1 doplňuje, že kromě KB není dostatečně financováno ani samotný obor IT. Také poukazuje na problém, že s postupem času není vynaložen dostatek peněz na další zlepšování. Podle respondenta č. 2 se situace s financováním KB pomalu zlepšuje, protože si organizace uvědomují, jaké rizika plynou z takové

hrozby. Větší problém, než financování vidí respondent v nedostatku odborníků. Stejného názoru je i respondent č. 4, který by byl pro větší podporu zaměstnanců a odborníků v téhle oblasti.

Tabulka 12 - Odpovědi k otázce č. 11 (zdroj: vlastní)

Otázka č. 11	
Spolupracujete při zajištění KB s jinými subjekty? Pokud ano, můžete uvést ty nejdůležitější a jejich význam?	
Odpovědi	
Respondent č. 1	*„Spolupracujeme s CESNETem a s NUKIBem."*
Respondent č. 2	*„Spolupracujeme, nicméně nemohu uvést nic konkrétního."*
Respondent č. 3	Nemocnice spolupracuje s NÚKIBEM
Respondent č. 4	*„Spolupracujeme s CESNETem – iniciativa hSOC a dále Provider služby."*

Otázka č. 11 se týkala spolupráce nemocnice při zajišťování kybernetické bezpečnosti. Dva respondenti uvedli spolupráci s NÚKIBem, k tomu respondenti č. 2 a 4. ještě doplňují spolupráci s CESNETem. Podrobnější informace o spolupráci respondenti nemohli uvést.

Tabulka 13 - Odpovědi k otázce č. 12 (zdroj: vlastní)

Otázka č. 12	
Existuje podle Vás univerzální řešení zabezpečení kybernetické bezpečnosti nemocnic?	
Odpovědi	
Respondent č. 1	*„Zatím ne, možná ani nikdy nebude, protože každá nemocnice je něčím specifická. Určitě by ale šla zpracovat nějaká univerzální „šablona“, která by se poté optimalizovala dle konkrétního zařízení.“*
Respondent č. 2	*„Univerzální recept na bezpečnost neexistuje, vnímal bych ovšem jako pozitivní vytvoření povinných bezpečnostních standardů pro všechny nemocnice v ČR.“*
Respondent č. 3	Spíš ne. Pomohly by centralizované funkce (dohledový tým monitorování).
Respondent č. 4	*„Ne. Je potřeba znát prostředí dané nemocnice, protože všechny nemocnice nejsou stejné. Nelze aplikovat na všechny nemocnice stejné řešení.“*

Na otázku, zda existuje univerzální řešení zabezpečení nemocnic proti kybernetickém útoku se respondenti shodli, že spíše ne. Respondent č. 1 a 2. se shodují že ne, protože každá nemocnice je něčím specifická. Respondent č. 2 si též myslí, že univerzální recept na bezpečnost neexistuje, avšak by mohly být vtvořený bezpečnostní standarty, které by každá nemocnice musela povinně dodržovat. Podle respondenta č. 1 by bylo možné zavést určité „šablony“, které by se přizpůsobily nemocnici a jejím potřebám a tato šablona by se musela dodržovat.

5.2 Celkové vyhodnocení informací získaných z rozhovorů

Téma stavu kybernetické bezpečnosti ve zdravotnických zařízeních a možnosti jejího zlepšení můžeme rozdělit na několik menších souvisejících témat. Hlavním předpokladem bezpečnosti v kyberprostoru je uvědomění si hrozícího nebezpečí, a to jak managementem organizace, tak jednotlivými zaměstnanci. Všichni respondenti kladou opakovaně důraz na vzdělávání všech osob, které pracují v rámci organizace s výpočetní technikou, komunikační a informační sítí. Toto téma se u respondentů mnohokrát opakuje, nicméně předpokladem zajištění vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti je management, který danou problematiku vnímá. V tomto ohledu nemají zdravotnická zařízení problém, neboť respondenti potvrzují, že management vnímá problematiku kybernetické bezpečnosti dostatečně. Toto tvrzení dokládá odpověď jednoho z respondentů: *„…náš management si problematiku kybernetické bezpečnosti uvědomuje, a proto bere každou kybernetickou hrozbu velmi vážně.“* Rozpor můžeme vnímat u respondenta č. 4, který má na danou problematiku jiný názor a to, že managment nemocnice tuto problematiku vnímá dle jeho slov „*nedostatečně*“. Současně se objevuje názor, že kybernetický útok provedený na jiné zdravotnické zařízení toto vnímání zvyšuje. Tvrzení je opět doloženo odpovědí respondenta: *„…pokud by nebylo útoků na jiné nemocnice, tak by kyberbezpečnost byla až na posledním místě. Nyní se doba změnila a vedení (nemocnice) tuto problematiku vnímá.“*

Těžiště kybernetické bezpečnosti je všemi respondenty vnímáno na poli edukace zaměstnanců. Jak říká jeden z respondentů: *„…první cestou jsou organizační opatření, zvyšování povědomí zaměstnanců o problematice kybernetické bezpečnosti.“* Zvyšování povědomí o možnostech kybernetického ohrožení je stejně jako u managementu spojeno s kybernetickými útoky na jiná zdravotnická zařízení: *„…po události v Benešově došlo ke vnímání problematiky a dopadů takového útoku mezi vedení i ostatními zaměstnanci.“* Edukace zaměstnanců pak probíhá na

dvou úrovních, což opět potvrzují všichni respondenti. Těmito úrovněmi jsou vstupní školení a pravidelné doškolení a sdílení aktuálních informací z oblasti kybernetické bezpečnosti: *„…každý nastupující zaměstnanec musí podstoupit školení v oblasti kybernetické bezpečnosti, kde je seznámen s možnými hrozbami, se kterými se lze setkat. Zaměstnancům jsou demonstrovány některé hrozby a jsou informování o tom, jak na ně reagovat.“* Kromě školení kybernetické bezpečnosti ještě probíhá: *„…školení na bezpečnost a ochrany zdraví při práci dvakrát ročně*“. Dále jsou pak zaměstnanci pravidelně informování o aktualitách buď prostřednicím porad nebo s využitím technických prostředků, například e-learning nebo intranet: *„…mimo nástupní školení se naši zaměstnanci vzdělávají v dané oblasti prostřednictvím e-learningového kurzu, který je vytvořen naším manažerem kybernetické bezpečnosti. E-learningový kurz obsahuje veškeré potřebné doporučení pro zodpovědné chování jedince při práci s informační komunikační technologií. Mimo veškerá školení jsou naši zaměstnanci informováni o aktuálních hrozbách z kyberprostoru každý týden v článku vypracovávaným naším manažerem kybernetické bezpečnosti.“*

Dalším zásadním tématem jsou pak konkrétní technická opatření, která mají kybernetickou bezpečnost zajistit. Respondenti se shodují, že základním technickým opatřením je používání antivirového programu a dále například firewallu, filtru spamu a nástroje pro monitoring síťového provozu a vyžadování dvoufaktorové autentizace: *„…technickým standardem je např. používání kvalitního spamfilteru, firewallu atd.“* Rozdíly pak můžeme pozorovat v konkrétních opatřeních přijímaných v souvislosti s konkrétní kybernetickou hrozbou. V případě phishingu nastává shoda, že jedinou účinnou obranou je poučený personál. Každý zaměstnanec by měl dokázat identifikovat podezřelý email a informovat o něm oddělení nebo osobu zodpovědnou za kybernetickou bezpečnost. I zde opětovně rezonuje řádná a pravidelná edukace, což potvrzují i respondenti: *„…klíčovým opatřením je správná a pravidelná edukace zaměstnanců o problematice Phishingu a Spearphisingu. Každý zaměstnanec by měl mít v paměti, že*

existuje něco jako Phishing a měl by být schopen ho na základě školení identifikovat." V případě ransomware útoku se již konkrétní opatření rozcházejí. První z respondentů uvádí opatření restriktivní: *„…zakázali jsme spouštění a instalaci aplikací uživatelům."* V případě druhého respondenta jsou zmíněna opatření spíše preventivní povahy, jako je například pravidelná záloha dat: *„…standardem je např.: provádění pravidelných záloh, používání kvalitního spamfilteru, Firewall, dodržování fyzické bezpečnosti, edukace zaměstnanců."*

Získaná data od jednotlivých respondentů však naznačují, že v oblasti zajištění kybernetické bezpečnosti existují také určitá slabá místa. Respondenti se shodují, že oblasti IT a zajištění bezpečnosti informačních a komunikačních systémů je nedostatečně financována a trpí nedostatkem odborníků, kteří jsou schopni kybernetickou bezpečnost ve zdravotnických zařízeních zajistit. Tyto problémy zmiňují respondenti opakovaně, například: *„…kyberbezpečnost je obecně podfinancována, totéž platí o IT."* *„Myslím si, že by jistě bylo vhodné financovat více."* Další respondent uvádí: *„…jako problém ovšem vnímám nedostatek odborníků v daném odvětví."* Poslední respondent odpovídá: *„…jako největší limit pro dosažení maximální možné kybernetické bezpečnosti vnímám nedostatečné množství odborníků v dané oblasti na trhu."*

Další slabinou se pak ukázal neexistující jednotný standard či postup, který by byl při zajišťování kybernetické bezpečnosti ve zdravotnických zařízeních povinně aplikován. Respondenti se kladně vyjadřují ke spolupráci a zejména k vydávaným doporučením ze strany Národního úřadu pro kybernetickou a informační bezpečnost, díky kterým mohou kybernetickou bezpečnost zvyšovat: *„…byla provedena opatření na základě doporučení NÚKIB."* I druhý a čtvrtý respondent uvádí následující: *„…spolupracujeme s CESNETem a s NUKIBem."* Respondenti nicméně souhrnně postrádají pevně definovaný minimální bezpečnostní standard: *„...univerzální recept na bezpečnost neexistuje, vnímal bych*

ovšem jako pozitivní vytvoření povinných bezpečnostních standardů pro všechny nemocnice v ČR.“ Ke stejné odpovědi se přiklání i čtvrtý respondent, která dodává: *„…Je potřeba znát prostředí dané nemocnice, protože všechny nemocnice nejsou stejné. Nelze aplikovat na všechny nemocnice stejné řešení.“*

5.3 Identifikace problémových oblastí

V případě kybernetického prostoru jsou spolu veškerá místa systému spojená, a proto nelze jednotlivě oddělit konkrétní problémové oblasti, ale jednotlivé problémové body jsou mezi sebou vzájemně provázané. Na základě vybraných případových studií a provedené kvalitativní analýzy lze konstatovat, že v případě zdravotnických zařízení je problémovou oblastí zajištění bezpečnosti proti útokům typu ransomware, protože tato zařízení zpracovávají a ukládají velká množství dat, hlavně těch osobních. Hlavní obranou proti ransomware útoku je zálohování, avšak neexistuje žádný zákon či předpis, který by zdravotnickým zařízením zálohování nařizoval, nebo určoval, jaký typ zálohy a s jakou pravidelností by mělo zdravotnické zařízení provádět. Dalším typem obrany je poté například řízený přístup ke složkám, ale ani v tomto případě neexistuje žádný jednotný postup či doporučující nastavení. Dále není nastavena jednotná kvalitativní úroveň zabezpečení serverů a pracovních stanic stejně jako úroveň kvality antivirových programů a programů pro detekci ransomware. Není také zavedena možnost kontroly provádění aktualizací pracovních aplikací ani antivirových a detekčních programů. K napadení komunikačního a informačního systému virem typu ransomware dohází nejčastěji otevřením infikované internetové stránky. Pro zdravotnická zařízení však neexistuje žádný doporučující seznam podezřelých webů, případně standardizované postupy zabezpečení emailové komunikace. Není-li útok cílený, využívá se k zavlečení škodlivého kódu phishingová kampaň. Zranitelným místem systému (zdravotnického zařízení) se poté stává každý pracovník s nízkou úrovní znalostí v oblasti kybernetické bezpečnosti stejně tak, jako špatně zabezpečený

informační a komunikační systém. Problémem je neexistující jednotná úroveň školení v oblasti kybernetické bezpečnosti, které musí každý zaměstnanec zdravotnického zařízení absolvovat. S ohledem na neustále se měnící typy kybernetických hrozeb a způsobů jakými lze systém napadnout, je další slabinou absolvování pouze vstupního školení bez stanovených intervalů, ve kterých je nutné školení aktualizovat a pro zaměstnance opakovat Edukace zaměstnanců i technické zabezpečení počítačové sítě je úzce spjato s financováním organizace, které může obě zmíněná témata limitovat. Otázka financování zdravotnických zařízení je však nad rámec této práce.

Jako slabé místo zajištění kybernetické bezpečnosti ve zdravotnických zařízeních po technické stránce lze identifikovat chybějící standard zabezpečení informačních a komunikačních sítí. Na začátku kapitoly bylo zmíněno, že se jednotlivé problémové oblasti překrývají a doplňují což je možno ilustrovat právě na tomto chybějícím jednotném standardu zabezpečení. Pokud by takový standard existoval, bylo by možno do něj zahrnout všechny výše zmíněné problémové oblasti. Tedy například zálohování dat stejně jako způsob, jak má zálohování probíhat a kam mají být zálohovaná data uložena. Dále povinnou aktualizaci softwarového vybavení a postih za užívání neaktuálního software, zejména operačních systémů pracovních stanic a serverů a softwarů pro detekci a ochranu před počítačovými viry. Současně s těmito technickými požadavky by bylo možno uvést obsahovou náplň a pravidelnost školení v oblasti kybernetické bezpečnosti bez ohledu na to, na kterém oddělení zdravotnického zařízení pracují.

5.4 Návrhy na zlepšení

S ohledem na identifikované nedostatky v oblasti zajištění kybernetické bezpečnosti zdravotnických zařízení, navrhuje tato práce vytvoření minimálního bezpečnostního standardu pro zdravotnická zařízení. Každý bezpečnostní

standard by musel být přizpůsobený danému zdravotnickému zařízení, protože jak již už bylo zmíněno, všechny nemocnice a zdravotnická zařízení mají určitá specifika. Při dodržení základních stejných zásad by bylo možno zajistit určitou standardizovanou úroveň bezpečnosti napříč zařízeními. Základem pro vznik tohoto standardu by se mohlo stát Doporučení NÚKIB pro administrátory. V současné době je na stránkách Národního úřadu pro kybernetickou a informační bezpečnost zveřejněna čtvrtá aktualizovaná verze tohoto doporučení. Doporučení je určeno manažerům kybernetické bezpečnosti, vedoucím pracovníkům IT oddělení a ostatním osobám, které se zajímají o kybernetickou bezpečnost v praktické rovině. Doporučení obsahuje konkrétní postupy k zabezpečení informační a komunikační sítě. Mezi doporučeními nechybí například zálohování důležitých dat včetně umístění zálohy mimo produkční síť, což je příklad konkrétního opatření, které může snížit vzniklé škody při útoku typu ransomware. Základním opatřením, které může přímo zabránit provedení kybernetického útoku, je nejen pravidelná, ale zejména včasná aktualizace veškerého software v rámci celé organizace. S ohledem na závažnost, jakou může zastaralý software způsobit by bylo vhodné vytvořit metodiku, která by se zabývala údržbou softwarů. Její dodržování by kontrolovalo přímo ministerstvo zdravotnictví nebo zřizovatelé nemocnic či jiných zdravotnických zařízení. V této metodice by bylo stanoveno, jakým způsobem a v jakých časových intervalech by bylo potřeba software aktualizovat.

Důležitou součástí ochrany proti kybernetickým hrozbám se doporučuje provádění pravidelných penetračních testů, které odhalí slabá místa v systému. Povinné provádění těchto testů či alespoň skenování zranitelností. Jejich provádění by mělo být vyžadováno z úrovně ministerstev a zřizovatelů zdravotnických zařízení.

Současně by mohl existovat speciální tým zřízený ministerstvem zdravotnictví, který by prováděl nejen namátkové kontroly dodržování nutných zásad kybernetické bezpečnosti, ale zjištěné nedostatky by byl schopen po technické stránce řešit na místě ve spolupráci se správcem komunikační a informační sítě daného zdravotnického zařízení.

V otázce záloh by ministerstvo zdravotnictví mohlo podpořit v rámci každého kraje vznik datového skladu, kde by byla povinně uložena veškerá provozní a další důležitá data všech oblastních nemocnic a krajské nemocnice nacházející se na území daného kraje, potažmo i fakultních nemocnic, pokud se v daném kraji vyskytují. Tento datový sklad by nebyl součástí žádné nemocnice či jiných zdravotnických zařízení. Tím by plnil roli zálohy umístěné mimo síť zdravotnického zařízení. Data by musela být pravidelně zálohována a ukládána do tohoto datového skladu např. jednou týdně, avšak v nepravidelných časech, tak aby útočník nemohl vysledovat, jaký den v týdnu v datovém skladu chybí nejvíce dat za uplynulé období. Současně by při tomto stavu zálohování bylo možné kontrolovat, zda opravdu nemocnice tyto data zálohují pravidelně a včas.

Podkapitolu navrhovaných opatření uzavírá návrh k nejvíce problematickému místu, kterým je správná edukace zaměstnanců a všech osob pracující v daném zdravotnickém zařízení s jakýmkoli zařízením, které je ke komunikační a informační síti připojeno. K zajištění dostatečného povědomí o kybernetických hrozbách je proto bezpodmínečně nutné, aby důkladným školením kybernetické bezpečnosti procházeli pravidelně všichni zaměstnanci, nikoli pouze osoby pracující na úseku komunikačních a informačních systémů. Důležité je zvyšování povědomí zaměstnanců o kybernetické bezpečnosti a nových trendech v této oblasti formou periodicky opakujících se školení. Také by bylo dobré obměňovat příklady kybernetických hrozeb ve školících materiálech a zaměstnance pravidelně testovat formou např. zasíláních

podvodných e-mailů připravených ze strany managmentu kybernetické bezpečnosti daného zdravotnického zařízení.

Zajímavou alternativou ke školení a rozesílání e-mailů obsahující phishingovou kampaň by bylo provádění bezpečnostních auditů zaměřených na uzamykání počítačů (např. počítačů na sesternách) při jejich ponechání bez dozoru, tak aby k nim neměly přístup neoprávněné osoby. Tyto audity by byly založené na vyčleněné skupině pracovníků nemocnice nebo ministerstva zdravotnictví (v závislosti na tom, zdali by se jednalo o interní nebo externí audit), kdy tito zaměstnanci, by měli za úkol procházet nemocniční oddělení se zaměřením na vyhledávání neuzamčených počítačů nebo jiných výpočetních systémů, které byly ponechány bez dozoru. V případě zjištěných nedostatků by bylo s daným zaměstnancem toto pochybení řešeno formou předání edukativního materiálu a v případě opakovaných prohřešků, např. formou sankcí ze strany zaměstnavatele.

6 DISKUZE

Kybernetické útoky mají v posledním desetiletí stoupající tendenci. Častým cílem těchto útoků jsou zdravotnická zařízení, která vzhledem k povaze jejich zaměření lze útokem vedeným proti zdravotnickému zařízení dosáhnout dopadů značného rozsahu. Toto je jeden z důvodů proč si útočníci vybírají nemocnice za svůj cíl. Dalším důvodem může být, že až donedávna kybernetická ochrana zdravotnických zařízení nebyla tolik řešena, a až v souvislosti s proběhlými útoky na obdobná zařízení, jak v rámci ČR, tak i v zahraničí začala být této problematice věnována pozornost.

Práce se proto zaměřila na zmapování zabezpečení informačních a komunikačních systémů zdravotnických zařízení před případnými kybernetickými útoky. Cílem práce bylo identifikovat zranitelná místa a navrhnout opatření ke zlepšení kybernetické bezpečnosti zdravotnických zařízení.

Obecně skokový nárůst kybernetických incidentů útoků byl zaznamenán v roce 2020 oproti roku 2019, což potvrzují i statistické údaje ze Zprávy o stavu kybernetické bezpečnosti České republiky za rok 2020 a následně za rok 2021. Tuto zprávu každoročně vydává NÚKIB. Níže uvedená tabulka zobrazuje počty nahlášených incidentů NÚKIBu za rok 2019, 2020 a 2021 [51, 52, 53]. Zpráva o incidentech v roce 2022 nebyla doposud vydána.

Tabulka 14 - Přehled počtu incidentů v letech 2019–2021 (zdroj dat: 50, 51, 52; zdroj tabulky: vlastní)

Rok	2019	2020	2021
Počet incidentů	217	468	476

Kromě nárustů kybernetických incidentů stoupla i kybernetická kriminalita. Velký nárůst trestných činů byl v roce 2021, kdy bylo řešeno 9518 trestných činů související s kybernetickou kriminalitou, kdy oproti tomu roku 2020 bylo řešeno 8073 činů [52, 53].

Co se týče samotného zdravotnictví, i zde došlo k nárustu útoků. Je zde patrná obecně stoupající tendence mezi lety 2019 a 2021, kdy v roce 2019 se odehrálo 6 útoků a v roce 2020 to bylo 16 útoků [52]. V roce 2021 počet opět stoupl na 26 útoků. Data za rok 2022 nyní ještě nejsou k dispozici, ale je možné předpokládat, že počet útoků i v tomto roce bude mít vzestupnou tendenci z důvodu událostí na Ukrajině. I ve světě rapidně stoupl počet kybernetických útoků [54]. Dle mého názoru měla pandemie COVID-19 značný podíl na zvýšení útoků i kyberkriminality.

Z rozhovoru s odborníky a následné analýzy odpovědí vyšlo několik klíčových okruhů, které jsou důležité pro kybernetickou bezpečnost zdravotnických zařízení. Prvním z těchto okruhů, který se často u respondentů opakoval byl nedostatek kvalifikovaného personálu, ať už se jednalo o specialisty zaměřené na kybernetickou bezpečnost, tak i IT specialisty. Že kybernetická bezpečnost dlouhodobě trpí nedostatkem specialistů potvrzuje i Zpráva o kybernetické bezpečnosti České republiky za rok 2019, 2020 a 2021 [51, 52, 53]. Zpráva z roku 2019 dokonce uvádí, že sektor zdravotnictví trpí největším nedostatkem specialistů a odborníků na KB [51]. Troufám si tvrdit, že nedostatkem odborníků bude zdravotnictví strádat ještě několik let. Hlavním důvodem může být, že státní sféra nedokáže tak dobře zaplatit IT specialisty či odborníky kybernetické bezpečnosti jako sféra soukromá.

Druhý okruh, na kterém se všichni respondenti shodli, je podfinancovaná kybernetická bezpečnost. Toto tvrzení opět dokládá jako u předchozího okruhu Zpráva o KB v ČR z let 2019, 2020 a 2021. Podfinancování je systémový problém, a proto nelze navrhnout žádné opatření, které by tento problém mohlo vyřešit. Jediný, co lze k financím říci je, že prevence je levnější než represe.

Dalším okruhem jsou technická opatření. Mezi ty se řádí používání antivirových programů, firewallů, filtrů spamu atd. Ale je důležité používat nové, aktualizované programy a ne zastaralé, protože by to mohlo spíš uškodit.

Poslední nejdůležitější oblastí je školení a vzdělávání zaměstnanců. Pokud má daná organizace, v našem případě zdravotnické zařízení, správně proškolený personál je nižší pravděpodobnost vzniku KÚ. Z výše uvedených konkrétních příkladů útoků na nemocnice lze vydedukovat, že člověk je nejslabší článek celé kybernetické bezpečnosti. A proto je důležité dbát zvýšenu pozornost školení zaměstnanců. Návrhem na vylepšení vzdělávání zaměstnanců je častější školení či semináře/přednášky týkající se kybernetické bezpečnosti. Nemyslím si, že samotné ústní školení stačí. Je potřeba to doplnit nějakou praktickou ukázkou. Proto personálu a zaměstnancům by bylo vhodné ukazovat různé podvodné e-maily se zaměřením, jak je rozeznat. Při školení by bylo potřeba se více zaměřit na časté chyby, kterých se zaměstnanci dopouští. Pro ověření znalostí zaměstnanců by mohly být IT specialistou nemocnice rozesílány „podvodné e-maily“ personálu. Touhle cestou by pak šlo vyhledat osoby, které nedodržely zásady ze školení a případně s nimi řešit další kroky.

Z vlastní zkušenosti jsem se setkala během praxí v nejmenované krajské nemocnici s častým ponecháváním odemčených počítačů bez dozoru, např. na sesternách. Takto ponechané počítače bez dozorů jsou vstupní bránou pro napadení systému jakýmkoliv typem m malware. Z tohoto důvodu je důležité se

kromě zaměření na školení kybernetických hrozeb zaměřovat i na školení obecného bezpečnostního povědomí, tak aby zaměstnanci věděli nejen jak rozpoznat škodlivé programy, ale také aby svým chováním neumožnili případnému útočníkovi snadný přístup do systému.

Nedostatkem této práce vnímám málo respondentů. Pokud by bylo více respondentů, mohlo by častěji docházet k různým názorům, čímž by se mohlo dojít i k jiným výsledkům. Avšak pro účely této práce je tento vzorek dostačující. Dalším nedostatkem vnímám otázku č. 9, kterou jsem špatně formulovala, jelikož ne všichni respondenti měli svého zřizovatele ministerstvo zdravotnictví.

7 ZÁVĚR

Hlavním úkolem bakalářské práce bylo mapování současného stavu ochrany nemocnic před kybernetickými útoky a na základě zjištěných skutečností identifikovat a navrhnout opatření na zlepšení současného stavu.

Teoretická část této práce představila legislativní rámec, který reguluje chování v kybernetickém prostoru. Následně byly vymezeny základní pojmy v oblasti kybernetické bezpečnosti. V této části byly rozepsány specifické znaky ohrožení útoků mířených na zdravotnická zařízení. Poslední kapitola popisovala případy útoků vedených na nemocnice jak v ČR, tak v zahraničí.

V praktické části byl vytvořena sada otevřených otázek na rozhovor určená konkrétním respondentům, kterými jsou osoby zapojené do zajištění kybernetické bezpečnosti v několika zdravotnických zařízeních. Otázky se týkaly současného stavu zajištění kybernetické bezpečnosti jak po stránce technické, tak po stránce personální.

Analýzou získaných odpovědí lze dovodit, že nelze dosáhnout stoprocentního zabezpečení proti kybernetickému útoku, nicméně práce navrhuje konkrétní opatření, kterými lze tato zabezpečení zvýšit. Těmito opatřeními jsou stanovení minimální bezpečnostního standardu pro zdravotnická zařízení vycházejícího z minimálního bezpečnostního standardu pro organizace nespadající pod regulaci zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Druhým opatřením je pak aktualizace doporučení Národního úřadu pro kybernetickou a informační bezpečnost pro administrátory informačních a komunikačních systémů. Osobám zodpovědným za zajištění kybernetické bezpečnosti ve zdravotnických zařízeních lze doporučit, aby oba tyto dokumenty, případně jejich aktualizované či přepracované verze, striktně dodržovali i za předpokladu, že jejich dodržování nebude vyžadováno zákonem.

8 SEZNAM POUŽITÝCH ZKRATEK

CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
ČR	Česká republika
DDoS	Distributed Denial of Service
DoS	Denial of service
EDR	Endpoint Detection and Response
EU	Evropská unie
FN	Fakultní nemocnice
IPA	Interpretativní fenomenologické analýza
IS	Informační systém
KB	Kybernetická bezpečnost
KI	Kritická infrastruktura
KII	Kritická informační infrastruktura
KÚ	Kybernetický útok
MITM	Man in the Middle
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost

SIEM	Security Information and Event Management
VKB	Vyhláška o kybernetické bezpečnosti
VPN	Virtuální privátní síť
ZKB	Zákon o kybernetické bezpečnosti

9 SEZNAM POUŽITÉ LITERATURY

[1] SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

[2] ČESKÁ REPUBLIKA. Zákon č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Zákony pro lidi* [online]. AION CS s.r.o., 2010-2023 [cit. 2023-04-21]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

[3] Legislativa KB. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost, 2023 [cit. 2023-04-21]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

[4] SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. In: Úřední věstník Evropské unie. Brusel, L 194/1, 19.7.2016. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=cs

[5] PAČKA, Roman. *CSIRT: v přední linii boje proti kybernetickým hrozbám*. Brno: Centrum pro studium demokracie a kultury, 2019. Politologická řada. ISBN 978-80-7325-473-5.

[6] Přichází směrnice NIS 2 a s ní revoluce v oblasti kybernetické bezpečnosti. *EPRAVO.CZ* [online]. Praha: Praha: epravo.cz, 2023, 30. 1. 2023, **1**(2023), 1 [cit. 2023-04-21]. ISSN 1213-189X. Dostupné z: https://www.epravo.cz/top/clanky/prichazi-smernice-nis-2-a-sni-revoluce-voblasti-kyberneticke-bezpecnosti-115821.html

[7] ČESKÁ REPUBLIKA. Vyhláška č. 82/2018 Sb., Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: *Zákony pro lidi* [online]. AION CS s.r.o., 2010-2023 [cit. 2023-04-21]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82

[8] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Páté doplněné a upravené vydání. Praha: Česká pobočka AFCEA, 2022. ISBN 978-80-908388-4-0.

[9] KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-34-8.

[10] Kybernetický útok (kyberútok). Definice, typy, následky a prevence. *LEGI§LATIVA* [online]. Praha: Legislativa s.r.o, 2023, 13.09.2022 [cit. 2023-04-22]. Dostupné z: https://legislativa.cz/zdroje/kyberneticka-bezpecnost/kyberneticky-utok

[11] Vyšší moc (vis maior). *AZlegal, advokátní kancelář* [online]. Praha: AZ LEGAL, advokátní kancelář, 2022 [cit. 2023-04-23]. Dostupné z: https://azlegal.cz/pravni-slovnik/vyssi-moc-vis-maior/

[12] HRŮZA, Petr. *Kybernetická bezpečnost II*. Brno: Univerzita obrany, 2013. ISBN 978-80-7231-931-2.

[13] Jak se bránit hackerům: Útoky typu DDoS jsou běžnou součástí digitálního světa, spolehlivá ochrana neexistuje. *Respekt* [online]. 10. 3. 2013 [cit. 2023-04-23]. ISSN 1801-1446. Dostupné z: https://www.respekt.cz/respekt-hub/jak-se-branit-hackerum

[14] Nejslavnější hackeři světa: Začali útočit už v dětském věku!. *EpochaPlus* [online]. RF-Hobby, 2023, 14.11.2017 [cit. 2023-04-23]. Dostupné z: https://epochaplus.cz/nejslavnejsi-hackeri-sveta-zacali-utocit-uz-v-detskem-veku/

[15] CHAŁUBIŃSKA-JENTKIEWICZ, Katarzyna, Filip RADONIEWICZ a Tadeusz ZIELIŃSKI. *Cybersecurity in Poland: Legal Aspects* [online]. Warsaw: Springer Nature Switzerland, 2022 [cit. 2023-04-24]. ISBN 978-3-030-78551-2. Dostupné z: https://link.springer.com/chapter/10.1007/978-3-030-78551-2_2

[16] Kdo je to vlastně ten HACKER?. *ISVS.CZ | Aktuálně to nejdůležitější o ISVS a eGovernmentu zde na jednom místě.* [online]. Týn nad Vltavou: ISVS.cz, 2023, 30.7.2021 [cit. 2023-04-24]. ISSN 1802-6575. Dostupné z: https://www.isvs.cz/kdo-je-to-vlastne-ten-hacker/

[17] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

[18] Riziko útoků na kritickou infrastrukturu roste. Nejhůře jsou zabezpečeny nemocnice, tvrdí asociace. *Česká televize: ČT 24* [online]. Praha: Česká televize, 2021, 25. 6. 2022 [cit. 2023-04-29]. Dostupné z: https://ct24.ceskatelevize.cz/domaci/3511096-riziko-utoku-na-kritickou-infrastrukturu-roste-nejhure-jsou-zabezpeceny-nemocnice

[19] Útoky hackerů na nemocnice sílí. Umírají kvůli nim lidé. *Seznam Zprávy* [online]. Praha: Seznam Zprávy, 2023 [cit. 2023-04-29]. Dostupné z: https://www.seznamzpravy.cz/clanek/fakta-utoky-hackeru-na-nemocnice-sili-umiraji-kvuli-nim-lide-217153

[20] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. ISBN 978-80-247-1561-2.

[21] *Kybernetická kriminalita v roce 2021 očima státního zastupitelství* [online]. In: . CZ.nic, 2023, 28.7.2022 [cit. 2023-04-30]. ISSN 2533-4727. Dostupné z: https://blog.nic.cz/2022/07/28/kyberneticka-kriminalita-v-roce-2021-ocima-statniho-zastupitelstvi/

[22] Strategie prevence kriminality v České republice na léta 2022-2027 [online.] Ministerstvo vnitra ČR, 2022. [cit. 2023-04-30]. Dostupné z: https://www.mvcr.cz/clanek/strategie-prevence-kriminality-v-ceske-republice-na-leta-2022-az-2027.aspx

[23] Phishing: definice phishingu, jak jej rozpoznat a jak na phishingový útok vyzrát. *Cnews.cz* [online]. Internet Info, 2023, 3.3.2022 [cit. 2023-05-02]. Dostupné z: https://www.cnews.cz/co-je-phishing-a-jak-se-branit

[24] Ransomware. *ESET* [online]. ESET, spol. s r.o., © 1992 – 2023 [cit. 2023-05-02]. Dostupné z: https://www.eset.com/cz/ransomware/

[25] DDoS útok. *ESET* [online]. ESET, spol. s r.o., © 1992 – 2023 [cit. 2023-05-02]. Dostupné z: https://www.eset.com/cz/ddos-utok/

[26] Smishing vs. Phishing: Differences, Similarities, and How to Prevent. *Perception Point* [online]. Boston, USA: Perception Point, 2023 [cit. 2023-05-03]. Dostupné z: https://perception-point.io/guides/phishing/smishing-vs-phishing-differences-similarities-and-how-to-prevent/

[27] Hacker způsobil benešovské nemocnici škodu 59 milionů, policie ho nedopadla. *IDnes.cz* [online]. Praha: MAFRA, 2023, 18. srpna 2020 [cit. 2023-05-

[05]. Dostupné z: https://www.idnes.cz/praha/zpravy/kyberneticky-utok-policie-vysetrovani-benesovska-nemocnice.A200818_090949_praha-zpravy_pp

[28] Nemocnice pod náporem hackerů: Jak proběhly nejznámější kyberútoky na české nemocnice?. *Avast* [online]. Praha: Avast Software, 1988 - 2023, 29.4.2021 [cit. 2023-05-05]. Dostupné z: https://blog.avast.com/cs/nemocnice-pod-naporem-hackeru-jak-probihaji-kyberutoky-na-ceske-nemocnice

[29] FN Brno se stala terčem kybernetického útoku. *Zdravotnický deník* [online]. Praha: Media Network, 14.3.2020 [cit. 2023-05-05]. Dostupné z: https://www.zdravotnickydenik.cz/2020/03/fn-brno-se-stala-tercem-kybernetickeho-utoku/

[30] Hacker, který podnikl masivní útok na druhou největší nemocnici v zemi, policii unikl. *Aktuálně.cz* [online]. Economia, 1999 – 2023, 1. 7. 2022 [cit. 2023-05-05]. Dostupné z: https://zpravy.aktualne.cz/domaci/kyberutok-nemocnice-odlozeno/r~ad936578f7b911ec8b4e0cc47ab5f122/

[31] Hackerským útokům čelily v Česku nemocnice, Národní knihovna či volební web. *Novinky.cz* [online]. Praha: Borgis, 2023, 21. 4. 2022 [cit. 2023-05-05]. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-hackerskym-utokum-celily-v-cesku-nemocnice-narodni-knihovna-ci-volebni-web-40394428

[32] The Düsseldorf Cyber Incident. *Institute for Peace Research and Security Policy at the University of Hamburg* [online]. Hamburg, Germany: Institute for Peace Research and Security Policy at the University of Hamburg, 09/30/20l20 [cit. 2023-05-05]. Dostupné z: https://ifsh.de/en/news-detail/the-duesseldorf-cyber-incident

[33] Duesseldorf University Hospital cyberattack leads to death of patient. *Verdict* [online]. © Verdict Media Limited 2023, © 2023, 18.9.2020 [cit. 2023-05-05]. Dostupné z: https://www.verdict.co.uk/duesseldorf-university-hospital-cyberattack/

[34] *Regulace kybernetického prostoru a kybernetická bezpečnost* [online]. Praha: EPRAVO.CZ, © 1999- [cit. 2023-05-05]. ISSN 1213-189X. Dostupné z: https://www.epravo.cz/top/clanky/regulace-kybernetickeho-prostoru-a-kyberneticka-bezpecnost-111871.html

[35] Vládní CERT. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Národní úřad pro kybernetickou a informační bezpečnost [cit. 2023-05-05]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/

[36] CZ.NIC-CSIRT. *Cz.nic: Správce domény cz* [online]. Praha: CZ.NIC, © 2023 [cit. 202 -05-05]. Dostupné z: https://www.nic.cz/csirt/

[37] 2. Koho se nové povinnosti týkají. *Národní úřad pro kybernetickou a informační bezpečnost: Vítejte na vzdělávacím portálu NÚKIB* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost [cit. 2023-05-06]. Dostupné z: https://osveta.nukib.cz/mod/page/view.php?id=2583

[38] Information system for bussines and beyond. *Pressbooks* [online]. Montreal: Pressbooks, © 2023 [cit. 2023-05-08]. Dostupné z: https://pressbooks.pub/bus206/chapter/chapter-1/

[39] *Varování* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost, 2020 [cit. 2023-05-09]. Dostupné z: https://www.nukib.cz/download/uredni_deska/Varovani_NUKIB_2020-04-16.pdf

[40] ČESKÁ REPUBLIKA. Zákon č. 240/2000 Sb., Zákon o krizovém řízení a o změně některých zákonů (krizový zákon). In: *Zákony pro lidi* [online]. AION CS s.r.o., 2010-2023 [cit. 2023-05-09]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-240

[41] Malware. *Avast* [online]. Avast Software, 1988–2023 [cit. 2023-05-11]. Dostupné z: https://www.avast.com/cs-cz/c-malware

[42] Malware. *ESET* [online]. í ESET, spol. s r.o, © 1992 – 2023 [cit. 2023-05-11]. Dostupné z: https://www.eset.com/cz/malware/

[43] WLAZLO, Patrick, Abhijeet SAHU, Zeyu MAO, Hao HUANG, Ana GOULART, Katherine DAVIS a Saman ZONOUZ. Man-in-the-middle attacks and defence in a power system cyber-physical testbed. *The Institution of Engineering and Technology* [online]. 2021, **6**(3), 164-177 [cit. 2023-05-11]. ISSN 2398-3396. Dostupné z: doi:10.1049/cps2.12014

[44] MITM (Man in the middle). *Digitální pevnost* [online]. Digitální pevnost, © 2018 [cit. 2023-05-11]. Dostupné z: https://www.digitalnipevnost.cz/viki/mitm-man-middle

[45] DRMOLA, Jakub. Konceptualizace kyberterorismu. *Vojenské rozhledy* [online]. © 1991-2021, **2013**(2), s. 94 - 102 [cit. 2023-05-12]. ISSN 1210-3292. Dostupné z: doi:10.3849/2336-2995.22.2013.02.094-102

[46] Police launch homicide inquiry after German hospital hack. *BBC.com* [online]. Londýn: BBC, © 2023, 18. září 2020 [cit. 2023-05-16]. Dostupné z: https://www.bbc.com/news/technology-54204356

[47] OLECKÁ, Ivana a Kateřina IVANOVÁ. *Metodologie vědecko-výzkumné činnosti*. Olomouc: Moravská vysoká škola Olomouc, 2010. ISBN 978-80-87240-33-5.

[49] Penetrační testování a vše kolem něj. *DoxoLogic* [online]. Praha: DoxoLogic, © 2023, 16.5. 2022 [cit. 2023-05-17]. Dostupné z: https://doxologic.cz/penetracni-testovani-a-vse-kolem-nej/

[50] Jaký je rozdíl mezi hardwarem a softwarem? *MyCom Solutions* [online]. Praha: MyCom Solutions, © 2023 [cit. 2023-05-17]. Dostupné z: https://mycom.cz/jaky-je-rozdil-mezi-hardwarem-a-softwarem/

[51] Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2019. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost [cit. 2023-05-18]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/NUKIB_ZSKB_2019.pdf

[52] Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost [cit. 2023-05-18]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf

[53] Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2021. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost [cit. 2023-05-18]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kybernetick_bezpenosti_2021.pdf

[54] *Počet kybernetických útoků na zdravotnická zařízení je meziročně zhruba stejný* [online]. ČTK, 2023 [cit. 2023-05-18]. ISSN 1213-5003. Dostupné z: https://www.ceskenoviny.cz/zpravy/2298806

[55] ŘIHÁČEK, Tomáš, Ivo ČERMÁK a Roman HYTYCH. *Kvalitativní analýza textů: čtyři přístupy*. Brno: Masarykova univerzita, 2013. ISBN 978-80-210-6382-2.

10 SEZNAM POUŽITÝCH OBRÁZKŮ

11 SEZNAM POUŽITÝCH TABULEK

12 SEZNAM PŘÍLOH

Příloha 1 – Otázky k rozhovoru

Otázky k praktické části BP

1. Jaká opatření a nástroje používáte pro zajištění kybernetické bezpečnosti v nemocnici?
2. Kolik osob má ve Vaší nemocnici na starost zabezpečení KB?
3. Jak vnímá kybernetické hrozby a z nich plynoucí rizika management Vaší nemocnice?
4. Jak zabezpečujete vzdělání zaměstnanců a personálu a jak často v oblasti kybernetické bezpečnosti?
5. Jaké konkrétní opatření používáte v souvislosti s obranou proti randsomware?
6. Jaké konkrétní opatření používáte v souvislosti s obranou proti phishingu?
7. Jaké změny byly ve vaší nemocnici provedeny po kybernetických útocích na nemocnice po kybernetických útocích na nemocnici v Benešově a na FN v Brně?
8. Jaké jsou podle Vás největší limity v oblasti kybernetické bezpečnosti nemocnice?
9. Jakými kroky vnímáte podporu ministerstva zdravotnictví a jiných vládních úřadů v posílení kybernetické bezpečnosti nemocnic?
10. Myslíte si, že je kybernetická bezpečnost dostatečně financována? Pomohlo by navýšení financí k lepšímu zabezpečení informačních systémů před kybernetickými útoky?
11. Spolupracujete při zajištění KB s jinými subjekty? Pokud ano, můžete uvést ty nejdůležitější a jejich význam?
12. Existuje podle Vás univerzální řešení zabezpečení kybernetické bezpečnosti nemocnic?