Aspekty kybernetické bezpečnosti v oblasti zdravotnictví

Marek Baláš

Bakalářská práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Marek Baláš**
Osobní číslo:	**L20003**
Studijní program:	**B1032A020002 Ochrana obyvatelstva**
Forma studia:	**Kombinovaná**
Téma práce:	**Aspekty kybernetické bezpečnosti v oblasti zdravotnictví**

Zásady pro vypracování

1. Zpracujte teoretický vstup do problematiky kybernetické bezpečnosti v kontextu onemocnění Covid-19.
2. Charakterizujte vybrané zdravotnické zařízení.
3. Proveďte vyhodnocení kybernetického útoku s důrazem na dopady pro zdravotnické zařízení.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. HONZÁK, Radkin, Karel DRBAL, Václav CÍLEK, et al. *Doba koronavirová*. Praha: Zeď, [2020], 305 s. ISBN 9788090767447.
2. MAREŠ, Miroslav, Jaroslav REKTOŘÍK a Jan ŠELEŠOVSKÝ. *Krizový management: případové bezpečnostní studie*. Praha: Ekopress, 2013, 237 s. ISBN 9788086929927.
3. STRUNECKÁ, Anna a Jiří PATOČKA. *Doba jedová a covidová*. Petrovice: ProfiSales, [2021], 318 s. ISBN 978-80-87494--38-7.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Lukáš Pavlík, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **1. prosince 2022**
Termín odevzdání bakalářské práce: **5. května 2023**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2022

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 5. 5. 2023

Jméno a příjmení studenta: Marek Baláš

.....
podpis studenta

ABSTRAKT

Bakalářská práce je tvořena teoretickou a praktickou částí. Teoretická část práce se zabývá problematikou koronavirů a onemocněním Covid–19. Jsou zde definována biologická ohrožení, popisuje krizové řízení, orgány krizového řízení a zmiňuje jednotlivé krizové plány. Dále je zde popsána oblast kybernetické bezpečnosti se zaměřením na charakteristiku kybernetických útoků a jejich dopadů na nemocniční prostředí. V praktické části je charakterizováno vybrané zdravotnické zařízení. Následně jsou uvedeny kybernetické hrozby phishing a ransomware a důvod jejich výběru je podložen statistickými údaji. Následuje řízený rozhovor s odborníkem na kybernetickou bezpečnost. Jsou zde analyzovány vybrané kybernetické hrozby vývojovými diagramy a určeny dopady na zdravotnické zařízení. Na dopady navazuje porovnání období Covid–19 a běžný stav. V závěru jsou vyhodnoceny výsledky a návrhy pro zlepšení.

Klíčová slova: Covid–19, krizové řízení, kybernetická bezpečnost, kybernetický útok, phishing, ransomware, vývojový diagram

ABSTRACT

The bachelor thesis consists of theoretical and practical parts. The theoretical part of the thesis deals with the issue of coronaviruses and the Covid-19 disease. It defines biological threats, describes crisis management, crisis management authorities and mentions individual crisis plans. Furthermore, the field of cyber security is described, focusing on the characteristics of cyber attacks and their impact on the hospital environment. In the practical part, a selected healthcare facility is characterised. Subsequently, the cyber threats phishing and ransomware are presented and the reason for their selection is supported by statistical data. This is followed by a guided interview with a cybersecurity expert. The selected cyber threats are analysed with flow charts and the impact is determined on healthcare facilities. The impacts are followed by a comparison of the Covid-19 period and the current state. Finally, the results are evaluated and suggestions for improvement are made.

Keywords: Covid-19, crisis management, cyber attack, cyber security, flow chart, phishing, ransomware

Tímto bych rád poděkoval panu Ing. Lukáši Pavlíkovi, Ph.D., za jeho vstřícnost, ochotu, konzultace a odborné vedení při zpracování bakalářské práce. Dále bych chtěl poděkovat odborníkům z oblasti kybernetické bezpečnosti za jejich rozhovor a poskytnuté informace. V neposlední řadě děkuji rodině a všem, kteří mě podporovali během studia.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Již od počátků vzniku počítačů bylo potřeba chránit tato zařízení proti neoprávněnému vniknutí. Od jednoduchých zabezpečení se postupně přecházelo k důmyslnějším a propracovanějším způsobům ochrany. Stejně jako se vyvíjela ochrana, vyvíjely se současně i hrozby. V současné době je kybernetická bezpečnost velmi diskutovaným tématem. Každé zařízení připojované k síti by mělo mít alespoň minimální ochranu před možnými kybernetickými hrozbami. Tyto hrozby mohou mít zanedbatelný vliv na zařízení, nebo naopak mohou způsobit velké potíže. Často způsobují špatnou funkci zařízení či krádež citlivých dat. Zásadní roli v oblasti kybernetické bezpečnosti hraje lidský faktor. Člověk je velmi často nejslabším článkem v zabezpečení celého systému. Jedním nepatrným kliknutím se následně může zhroutit celý systém organizace, firmy nebo instituce.

V březnu roku 2020 se v České republice začal šířit nový virus SARS–CoV–2. Tento koronavir se začal nekontrolovatelně šířit po celém světě, a zastihl tak spoustu lidí nepřipravených. Onemocnění způsobené tímto virem se začalo říkat Covid–19. Začala se zavádět přísná karanténní opatření a započal vývoj vakcín proti tomuto onemocnění. I přes přísná karanténní opatření se zdravotnická zařízení začala plnit lidmi mající těžký průběh onemocnění. Zdravotnický personál byl pod velkým tlakem a začal být jeho nedostatek. Přesouvaly se také operační zákroky, které nebyly prioritou. Postupem času byla na podporu zdravotnického personálu nasazena i Armáda České republiky, aby pomohla zdravotnickému personálu se zvládnutím těžké situace v nemocnicích. Na následky způsobené onemocněním Covid–19 zemřelo po celém světě téměř sedm milionů lidí.

Pandemie Covid–19 ovlivnila zdravotnická zařízení v mnoha oblastech. Zdravotnická zařízení napříč Českou republikou, která i před obdobím pandemie neměla dostatečně vysokou úroveň zabezpečení sítí a byl zde nedostatek kvalifikovaného personálu v oblasti informatiky, byla v tomto období vystavena velkému nátlaku. Během pandemie postihly kybernetické útoky spoustu organizací a nemocnice nebyly výjimkou. Tyto útoky měly za následek ochromení systému nebo úplné vyřazení systému z činnosti. Nemohlo se operovat a nešly přenášet informace do databázového systému. Nemocnice tyto útoky stály řádově desítky milionů korun a byly ohroženy životy pacientů z důvodu nefunkčnosti některých přístrojů. Doba do úplné obnovy systému může být v rozmezí měsíců i let. Pachatelé jsou často z ciziny a jde je velmi těžko dohledat. V konečném důsledku tedy nezbývá nic jiného než trestní řízení odložit.

Cílem bakalářské práce je zjistit, zda pandemie Covid–19 ovlivnila kybernetické útoky mířené na nemocniční zařízení. Vybrat kybernetické hrozby na základě statistických údajů ze světa i domova. Tyto hrozby dále analyzovat a provést vyhodnocení výsledků se zaměřením na teoretické dopady pro vybrané nemocniční zařízení. Porovnat období pandemie Covid–19 a běžný stav v oblasti kybernetické bezpečnosti. Vyhodnotit výsledky a provést návrh na zlepšení.

I. TEORETICKÁ ČÁST

1 KORONAVIRY

Koronaviry byly pojmenovány a pod tímto názvem označovány až v roce 1968, a to podle snímků z elektronového mikroskopu. Tyto viry, jenž zapříčiňují respirační onemocnění u ptáků a savců jsou jinak známé virology už od 30. let 20. století. Koronaviry mají okolo sebe „halo“ strukturu, která vypadá jako korona obklopující slunce. Tuto strukturu tvoří několik desítek spiků. SARS–CoV–2 jich má údajně v průměru 74 (Naqvi et al., 2020).

Až ve 21. století dva koronaviry měly vážný průběh nemoci u člověka. Šlo o **onemocnění SARS** (*Severe Acute Respiratory Syndrome–těžký akutní respirační syndrom*), jenž se poprvé vyskytlo roku 2003. Původcem tohoto onemocnění byl SARS–CoV virus. Zasaženo bylo přes 8 000 lidí obývajících 29 států a teritorií. Ze všech infikovaných zemřelo minimálně 774 osob. Území zasažená tímto virem zavedla striktní epidemiologická opatření a onemocnění následně zmizelo (Naqvi et al., 2020).

Značné znepokojení způsobilo roku 2012 **onemocnění MERS** (*Middle East Respiratory Syndrome–středněvýchodní respirační syndrom*). Zdrojem viru MERS–CoV byl shledán velbloud. Tomu byl virus předán netopýrem, stejně jako tomu bylo u viru SARS-CoV. Dokázalo se, že virus se může šířit z osoby na osobu a je u něj velká smrtnost. Saudská Arábie evidovala 124 případů nákazy a z toho 52 zemřelo. V Korejské republice se virus MERS objevil v květnu roku 2015. V roce 2019 byla oznámena velká smrtnost zapříčiněná tímto virem – 34,5 % (Naqvi et al., 2020; Hu et al., 2020; Rehman et al., 2020).

Podle světové zdravotnické organizace bylo ve světě zaznamenáno 2 442 případů infekcí virem MERS. Ze všech nakažených bylo následně cca 300–500 mrtvých. Byla zavedena striktní epidemiologická a hygienická opatření, která následně poté vedla k zastavení šíření tohoto infekčního onemocnění (Naqvi et al., 2020).

Počátkem roku 2020 bylo zjištěno, že virus SARS–CoV–2 se řadí mezi koronaviry. Spike proteiny, které se nachází na povrchu viru, jsou nejvíce známé a symbolické pro vzhled těchto nebezpečných koronavirů (Naqvi et al., 2020). Slovo „spike“ je anglické slovo užívající se i v českých publikacích a lékařské terminologii, např. spikové proteiny (Strunecká a Patočka, 2021).

1.1 Covid–19

První oficiální případy respiračního onemocnění Covid–19 se objevily v prosinci roku 2019. V tu dobu Čína oznámila, že virus byl přenesen na člověka netopýrem. První nakažení se měli infikovat ve městě Wu–chan na tržišti Chua–nan v provincii Chu–pej. V reakci na předchozí koronaviry se Čína rozhodla uzavřít 22. ledna 2020 nejvíce zalidněné město nacházející se ve střední Číně Wu–chan. Spolu s městem o počtu 11 milionů obyvatel byla uzavřena i provincie Chu–pej. Zdravotnictví a vlády na různých kontinentech a v mnoha státech byly nepřipraveny z důvodu rychle se šířícího viru počátkem roku 2020 (Strunecká a Patočka, 2021).

K 6. lednu 2023 bylo podle Světové zdravotnické organizace (dále jen „WHO“) celosvětově evidováno od počátku pandemie celkem 657 977 736 oficiálně potvrzených případů Covid–19. S tímto číslem je spojeno i 6 681 433 oficiálních úmrtí po celém světě. V boji proti tomuto onemocnění bylo k 22. prosinci 2022 celosvětově aplikováno celkem 13 073 712 554 dávek vakcín (WHO Coronavirus…, c2023).

Nejvíce nakažených bylo doposud evidováno ve Spojených státech amerických, a to s celkovým počtem 99 423 758 osob. Největší počet zemřelých v důsledku tohoto onemocnění je opět evidován ve Spojených státech amerických v počtu 1 082 265 osob od počátku pandemie (WHO Coronavirus…, c2023).

V České republice (dále jen „ČR“) bylo k 7. lednu 2023 evidováno 4 582 860 potvrzených případů od počátku pandemie, a to včetně reinfekcí, které tvoří celkově 378 983 případů. Počet úmrtí se v ČR vyšplhal k 6. lednu 2023 na 42 196 osob a k 7. lednu 2023 bylo celkově vykázáno 18 594 648 očkování (Onemocnění aktuálně, 2023).

1.2 Vir SARS–CoV–2 a Covid–19

Značná část celosvětové populace bude virem SARS–CoV–2 dříve či později infikována. Této skutečnosti nezabránila ani přísná karanténní opatření, která povedou pouze ke zpomalení šíření infekce. Karanténa zapříčiní také to, že pravděpodobnost styku osob s virem bude nižší. Z toho vyplývá větší náchylnost na další vlny viru, které mohou následovat, a to z důvodu absence kontaktu s virem z vln předchozích. Následkem infekce virem SARS–CoV–2 je pak onemocnění Covid–19 (Coronavirus disease 2019). V tomto onemocnění se již musí objevit některé klinické příznaky (Honzák et al., 2020).

Jen nízké procento obyvatelstva je onemocněním Covid–19 postihnuto a jen malé množství populace pozitivně testované na vir SARS–CoV–2 na onemocnění opravdu zemře. Počty potvrzených úmrtí se snižují, a nakonec se vyrovnají číslům rovnajícím se sezónní chřipce. Na chřipku v ČR zemře ročně několik tisíc lidí, celosvětově pak jde až o půl milionu. Avšak z 90 % jak u chřipky, tak i u onemocnění Covid–19 jde o úmrtí na následky bakteriálního zánětu, kterému chřipka či Covid–19 otevřely bránu do plic (Honzák et al., 2020).

1.3 Struktura SARS–CoV–2

Jde o částice kulovitého tvaru, které jsou obklopeny obalem a jsou v nich zakotveny obalové, spikové, membránové a nukleokapsidové proteiny. Jejich podobnost s bílkovinami SARS–CoV a MERS–CoV je vysoce sekvenační. V molekule jedno vláknové ribonukleové kyseliny je zakódována dědičná informace (RNA). Genomy koronavirů jsou jedny z největších ze všech RNA virů (26–32 kb na délku) (Naqvi et al. 2020).

Vir, šířící se Wu–chanem počátkem roku 2020 byl první celistvý genom koronavirusu SARS–CoV–2. To přineslo objev, že virová RNA je tvořena cca 30 000 písmeny genetického kódu, ve kterých je ukryta instrukce pro syntézu 27 virových proteinů. Do 3 subjednotek je uspořádáno 1 273 aminokyselin tvořící molekulu spikové bílkoviny SARS–CoV–2. Subjetnotka S1 slouží k zakotvení ve virovém obalu. Subjednotky S2 mají tvar V a zachycují se na povrchu buňky hostitele a množí se po průniku buňkou. ACE2 proteiny jsou receptory, se kterými se spojují spikové proteiny subjednotek S2. Aktivita proteinů ACE2 je ovlivňována léky na snížení krevního tlaku. Při rozkladu obalu koronaviru proteiny ACE2 působí společně a dovolují tak, aby se jeho RNA uvolnila do cytoplazmy buňky hostitele. Ta následně zapříčiní její množení a syntézu veškerých nezbytných bílkovin. V buňce hostitele (člověka) je skládáno spoustu nových virů. Do tělesných tekutin je pak buňkou uvolněna nová generace virů (Hu et al., 2020; Huang et al., 2020; Rehman et al., 2020).

1.3.1 DNA

Jde o látku, která se nachází ve veškerých buněčných organismech. Je v ní obsažena genetická informace, která říká, jak budou ať už rostliny, živočichové, bakterie či houby vypadat a jakým způsobem se budou odehrávat veškeré životní procesy určitého organismu. V případě rostoucího organismu dochází k dělení buněk (Trousilová).

V případě dělení jádra buňky se DNA replikuje. K tomu dochází z toho důvodu, aby nově vytvořená buňka obsahovala stejnou informaci.
DNA je tvořena třemi základními částmi:

- Zbytky kyseliny fosforečné.
- Molekulami deoxyribózy.
- Dusíkatými bázemi.

Spojením jednotlivých částí vzniká již známá dvojitá šroubovice (Trousilová).

1.3.2 RNA

Informace jsou předávány pomocí RNA – ribonukleových kyselin. DNA je podobná RNA, ta je však tvořena jen jedním vláknem. V případě některých virů funkci DNA nahrazuje RNA. Má se za to, že při vývoji života se RNA stala prvotním nositelem genetické informace a deoxyribonukleová kyselina byla vyvinuta časem (Trousilová).

Máme tři druhy RNA:

- Mediátorová RNA (mRNA).
- Transferová RNA (tRNA).
- Ribozomová RNA (rRNA) (Trousilová).

1.4 Symptomy Covidu–19

Nový typ pneumonie je charakterizován jako Covid–19, který je zapříčiněný infekcí koronavirem SARS–CoV–2. Po určité době je již jasné, že SARS–CoV–2 se chová ne zcela běžným a nepředvídatelným způsobem. Během roku 2020 bylo ověřeno, že spousta infikovaných nevykazuje příznaky nákazy. Tento průběh nákazy označujeme jako asymptomatický. Po infikování virem se u některých osob mohou vyskytnout jen mírné symptomy, avšak u jiných může jít o velice těžký průběh nemoci, který v krajních případech končí i smrtí. Osoby postihnuté onemocněním Covid–19 mají příznaky nemoci ve většině případů po 5–6 dnech. Není vyloučeno, že se příznaky projeví i po delší době. Může to být i po 14 dnech (Strunecká a Patočka, 2021).

Je uvedeno, že:

- přes 90 % nakažených trpí horečkami. Kontrola zvýšené teploty bezkontaktními teploměry se tak stala často používaným prvním testem pro zachycení nakažených osob,
- 50–76 % nakažených trpí suchým kašlem,
- 25–44 % nakažených je unaveno,
- je možné, že se také projeví i jiné symptomy. Těmi mohou být rýma, produkce hlenu, bolest hlavy, tíže na hrudi, bolest v krku nebo silné pocení,
- ztráta čichu a chuti je velice častým symptomem této nemoci,
- mohou se také objevit zduřené a zčervenalé koncové články prstů převážně na nohou. V tomto případě jde o tzv. covidové prsty,
- v současnosti je již jasné, že někdy dochází i k dlouhodobému postižení plic. I když se jedná o virus respirační, je prokázáno, že může napadat i mozek, ledviny, srdce a jiné orgány. Víme také, že SARS–CoV–2 způsobuje zvýšenou srážlivost krve. Má následky ledvinné a neurologické, a také ničí endotel cév,
- s dušností, únavou a bolestmi hlavy se mohou potýkat i lidé, kteří prodělali pouze lehký průběh nemoci, a to i po dobu několika týdnů (Strunecká a Patočka, 2021).

Z důvodu vysokého počtu hospitalizovaných a nakažených přibylo více symptomů této nemoci. V současné době k nim patří i zvracení, bolesti břicha, průjem, rychle rostoucí nehty, vyrážka a jiné (Hu et al., 2020; Jiang et al., 2020).

Co se týká statistických údajů, setkáváme se i s počtem úmrtí. Demografický ukazatel, který udává počet zemřelých za určité období z určité populace je úmrtnost (mortalita). Ta se vztahuje na celkové obyvatelstvo. Smrtnost (letalita) je naopak údaj, který ukazuje podíl úmrtí z celkového počtu nakažených. Ústav zdravotnických informací a statistiky ČR a Ministerstvo zdravotnictví ČR poskytují mimo jiné i informace a statistické údaje týkající se pandemie Covid–19 (Strunecká a Patočka, 2021).

1.5 Reprodukční číslo

Jde o číslo, které udává, kolik dalších lidí je schopen nakazit jeden již nakažený člověk. Pokud jeden nakažený pacient nakazí v průměru další 2 osoby, jenž nákazu šíří dále, pak je reprodukční číslo 2 (Májek, 2020).

Základní reprodukční číslo signalizuje prvotní hodnotu u daného obyvatelstva ještě před tím, než jsou zavedena ochranná opatření. Číslo by se mělo po přijetí určitých opatření snížit. **Efektivní reprodukční číslo** je hodnota vycházející z přijatých opatření a základního reprodukčního čísla. V tomto případě by již nemělo docházet k tak rychlému rozrůstání epidemie a počty nakažených by měly klesat (Májek, 2020).

Infekčnost nemocného je doba, ve které lze nemoc šířit a počet kontaktů, se kterými se nakažený za dobu své infekčnosti stýká, jsou jedny ze základních pilířů, jenž ovlivňují velikost reprodukčního čísla (Májek, 2020).

1.6 Vakcinace

Jako jedno z nejpravděpodobnějších možných řešení, jak zastavit Covid–19 vidí lidé včetně vlád a zdravotníků v očkování. Vychází tím z historických zkušeností, kde se očkováním předešlo jiným infekčním nemocem, úmrtím nebo poškozením zdraví u dětí i dospělých. Dříve bylo očkování považováno za samozřejmé a nežádoucím účinkům nebyla věnována velká pozornost. I očkovaní mohou nemoc prodělat, nebo patogeny šířit dál. Imunita po prodělaném očkování časem vyprchá. Prakticky celoživotní imunitu získá člověk jen v případech prodělání některých nemocí např. spalničky, zarděnky a vybrané typy chřipky.
Vývoj vakcíny probíhá běžně v preklinickém výzkumu v laboratoři a poté v několika dalších fázích. Po projití laboratorními podmínkami a testům na zvířatech se přechází na testování na lidech. Fáze jsou rozděleny do tří částí. V první fázi je vakcína podávána několika málo lidem. Ve druhé fázi jde o test u většího počtu osob. Tyto osoby odpovídají pohlavím, věkem i fyzickým charakterem cílovým skupinám. V poslední třetí fázi je vakcína podávána tisícům dobrovolníků. U těchto lidí se následně sleduje, jakým způsobem vakcína účinkuje a pozorují se také nežádoucí účinky. Obvykle jsou osoby sledovány po dobu 7 dnů. I přes to může dojít po podání vakcíny v plošném měřítku lidem jak zdravým, tak i nemocným k projevení závažných nežádoucích účinků (Strunecká a Patočka, 2021).
Už v srpnu 2020 byla uvedena první vakcína proti onemocnění Covid–19. Touto vakcínou byla ruská vakcína Sputnik V. U této vakcíny nebyly zveřejněny výsledky třetí fáze. Vakcína tedy není brána za spolehlivou (Strunecká a Patočka, 2021).

Evropská léková agentura (dále jen „EMA“) 21. prosince 2020 schválila vakcínu splňující požadavky Evropské unie (dále jen „EU“). Touto vakcínou byla Comirnaty konsorcia BioNTec–Pfizer a poté 6. ledna 2021 od americké firmy Moderna očkovací látka nesoucí stejný název (Strunecká a Patočka, 2021).

Tyto vakcíny jsou založeny na mRNA. Firmy BioNTech a Pfizer prohlásily, že mají v úmyslu vyrobit 1, 3 miliardy dávek za rok 2021. Vakcína byla schválena ve 22 zemích, např. ve Spojených státech amerických (dále jen „USA“) nebo Velké Británii. EU si objednala 300 mil. dávek a USA dalších 200 mil. (Strunecká a Patočka, 2021).

První očkující zemí v západní Evropě 8. prosince 2020 byla Velká Británie, která nebyla omezována schválením vakcíny EU. Koncem prosince 2020 se začalo očkovat stejně jako ve Velké Británii vakcínou BioNTech–Pfizer i v ČR. Mezi zápory této vakcíny patří nutnost skladovat ji při -70 °C (Strunecká a Patočka, 2021).

Firma moderna měla v plánu vyrobit nejméně 600 mil. dávek za rok 2021 s možností tento počet navýšit na 1 mld. EU si rezervovala 80 mil. dávek a USA 300 mil. dávek. Tuto vakcínu si také objednaly země jako je např. Japonsko a Švýcarsko. Mezi velké přednosti této vakcíny patří skladovatelnost při -20 °C až 6 měsíců. V lednici je schopná vydržet až 30 dní. Není nutnost ji jakýmkoliv způsobem ředit. Vakcíny jsou podávány dvěma dávkami s rozestupem 4 týdny (Strunecká a Patočka, 2021).

V lednu 2021 EMA oznámila obdržení žádosti na podmínečnou registraci na trhu EU vakcíny od Oxford–AstraZeneca a Oxfordské univerzity. Vakcína byla doporučena ke schválení a přijetí EU i přes vážné diskuse. Německé, rakouské, francouzské a švédské úřady doporučily očkování vakcínou jen u lidí do 65 let. Experty z WHO bylo uvedeno, že výhody vakcíny převažují nad riziky, a tak by se měli očkovat i lidé nad 65 let (Strunecká a Patočka, 2021).

Lze také použít léčiva, která jsou již známá a odzkoušená běžným užíváním k léčbě jiných chorob. Jde o tzv. repurposing, kdy se schválená látka využívá k jiným účelům. Tyto látky mohou být okamžitě nasazeny bez předchozího vývoje. Musí být ale vhodně a individuálně kombinovány dle stavu pacienta (Honzák et al., 2020).

1.6.1 mRNA vakcíny

Vakcíny typu mRNA se liší od vakcín používajících se doposud. Neobsahuje totiž mrtvý či oslabený virus. Je v nich obsažen genetický templát pro úsek SARS–CoV–2 viru v podobě mRNA. Vakcíny jsou určeny k tomu, aby naučily tělo rozeznat antigen způsobující onemocnění (Strunecká a Patočka, 2021).

Vakcíny RNA dávají tělu instrukce tak, že si patogenní antigen samo nasyntetizuje. Je však vyžadováno, že mRNA musí proniknout až do buněk člověka podstupujícího očkování a započít zde reakci imunitního systému (Strunecká a Patočka, 2021).
Možné užití mRNA v očkovacích látkách je diskutováno již prakticky 30 let. Proces vývoje těchto vakcín urychlila až narůstající poptávka po vakcínách v době pandemie Covid-19. Mezi pozitiva vakcíny patří její rychlost, díky které se může vytvořit pro různé patogeny. Do templátu DNA je vložena genetická sekvence patogenního viru, díky které je možnost nasyntetizovat spoustu odpovídající mRNA. Ta je následně použita pro přípravu vakcín.
Nástup pandemie Covid–19 je pro rozvoj genetických vakcín obrovský zlom. Nebylo jisté, zda se vynaložené finanční prostředky na vývoj vakcín vrátí, a tak si na mRNA vakcíny žádný netroufal. Teprve až po uvolnění financí ze strany sponzorů a jednotlivých zemí se vývoj vakcín mohl rozběhnout naplno. Tyto vakcíny jsou desetinásobně dražší než vakcíny s adenovirovými nosiči (Strunecká a Patočka, 2021).

1.6.2 Vektorové vakcíny

Tyto vakcíny fungují na principu využití neškodného adenoviru, který je nosičem genetické zprávy spikového proteinu SARS–CoV–2, na nějž by měla být vyvolána imunitní odpověď. Genom adenoviru je v podobě jedné molekuly dvouvláknové DNA. Do zmíněné molekuly je dána DNA kódující spikové proteiny. V této situaci je virus oslaben, aby se po vstoupení do buňky nemnožil (Strunecká a Patočka, 2021).

Jde o jakýsi obal, uvnitř jehož je genetická informace namísto lipidové nanopartikule užívané v mRNA vakcínách. Po proniknutí do buňky adenovirus uvolňuje dvojitou šroubovici DNA a následně dojde k přepisu na mRNA pomocí buněčných mechanismů příjemce vakcíny. Ta v buňce započne syntézu spikového proteinu, který uvolněním z buňky zpátky do krve plní funkci antigenu. Odlišnost je v tom, že u mRNA vakcíny je proces kratší, protože postrádá fázi přepisu DNA do mRNA. Zástupcem těchto vakcín je např. Oxford–AstraZeneca. Ta obsahuje adenovirový nosič, jenž u šimpanzů zapříčiňuje obyčejné nachlazení. Vakcína je podávána ve dvou dávkách v rozmezí 4 týdny a lze ji skladovat při teplotě 2–8 °C až 31 dní. Její velkou výhodou je cena pohybující se zhruba kolem 4 dolarů za kus (Strunecká a Patočka, 2021).

2 BIOLOGICKÁ OHROŽENÍ

Jedná se o přírodní mimořádné události. Tato ohrožení jsou zapříčiněna živou přírodou a mohou být při nich vážně ohrožena zvířata, lidé i rostliny. Mezi pohromy mající biologickou povahu patří epizootie, epifytie, epidemie a pandemie (Základní pojmy, c2022; Vránová, 2013).

2.1 Epizootie, epifytie, epidemie, pandemie

V případě **epizootie** se jedná o nakažlivé onemocnění zvířat s hromadným výskytem. Vyskytuje se v krátkých časových úsecích a na omezených prostorech. Obvykle jsou její počátky malé, avšak následně dochází k rychlému šíření i za hranice prvotního ohniska. Pojem panzootie označuje extrémní formu epizootie. Tato nákaza se šíří až lavinovým způsobem. Může v obrovském rozsahu postihnout několik druhů zvířat. Onemocnění je šířeno napříč kontinenty. Jedná se zde např. o slintavku a kulhavku nebo vzteklinu (Harnach, 1960).

U **epifytie** jde o hromadnou nákazu zemědělských plodin a lesních kultur. Příčina vzniku epifytií je závislá na klimatických podmínkách za období vegetace zemědělských plodin a na údajích, které jsou rychle a kvalitně zpracovávány z odborného posouzení nákaz v terénu. Dopad na epifytii má také ošetření plodin a velikost plochy, na které je plodina pěstována. K zamezení šíření epifytie zveřejňuje Státní rostlinolékařská správa informace o přítomnosti nepříznivých organismů a poruch, jež jsou zveřejňovány na webových stránkách. Tato Státní rostlinolékařská správa mimo jiné zabraňuje zavlečení organismů z jiných zemí a zamezuje šíření škodlivých organismů na daném území. V případě vzniku epifytie ji lze označit pouze jako mimořádnou událost (Pešan, 2010).

Epidemie se vyznačuje zvýšeným výskytem infekčního onemocnění. To je dáno specifikovanou oblastí a určitým časovým vymezením. O epidemii mluvíme v případě, že jde o infekční onemocnění mající vyšší výskyt nebo značné převýšení výskytu, než bylo očekáváno. U jednotlivých států se může definice značně převyšující výskyt měnit. Ta je dána ukazateli množství podaných léků, úmrtností, počtem nově nakažených a počtem lidí v pracovní neschopnosti (Pandemie vs epidemie, c2016–2022).

O **pandemii** mluvíme v případě infekčního onemocnění bez omezeného prostoru. Pandemie tedy vzniká v případě rozšíření se do okolních států či kontinentů. Onemocnění v rámci epidemie může ještě reagovat na léčbu, u pandemie však už nikoliv. Včasnou reakcí států a preventivními opatřeními je možné pandemii zamezit (Pandemie vs epidemie, c2016–2022).

2.2 Pandemický plán

Tento plán obsahuje pečlivá a v dostatečném předstihu připravená opatření, která jsou zavedena v případě vzniku pandemie. Zaváděná opatření mohou ve značném rozsahu zmírnit dopady pandemie (Pandemické plány, c2016–2022)..

Každý stát si své pandemické plány vytváří sám. Je tak prováděno z toho důvodu, že každá země je závislá na jiných podmínkách. Řídí se však doporučeními WHO. Tato organizace rozdělila postup pandemie do jednotlivých fází. Každá fáze obsahuje návod, který definuje, co dělat během dané fáze (Pandemické plány, c2016–2022).

2.2.1 Pandemický plán ČR

Jde o dokument, který ve svém obsahu stanovuje postupy a popisuje primární reakci ČR na vzniklou pandemii chřipky, již zapříčiňuje nový typ chřipkového viru. Jestliže vznikne pandemie chřipky, tak cílem tohoto plánu je zmírnění očekávaných sociálních, ekonomických a zdravotních následků (Pandemický plán ČR, 2011). Podklady, v jaké fázi se právě chřipka nachází, zajišťuje program sledování onemocnění (surveillance). V ČR se tímto programem zaobírají národní referenční laboratoře a Národní referenční centrum pro analýzu epidemiologických dat. Ty jsou dále doplňovány epidemiologickými odděleními a laboratořemi v krajích (Pandemické plány, c2016–2022)..
Informace o situaci v jiných státech jsou ministerstvu zdravotnictví poskytovány od WHO. Plán zahrnuje také aplikaci Pandemie. Jejím účelem je sdílet informace a koordinovat činnost napříč ČR (Pandemické plány, c2016–2022).

2.2.2 Pandemický plán rezortu zdravotnictví

Na Pandemický plán ČR navazuje Pandemický plán rezortu zdravotnictví. Byl vytvořen na Ministerstvu zdravotnictví roku 2012 (Pandemický plán rezortu zdravotnictví, 2012).

Jeho zásadní kapitoly tvoří:

- vakcinační strategie,
- komunikační strategie,
- činnosti orgánů ochrany veřejného zdraví,
- činnost poskytovatelů zdravotních služeb.

Součást plánu tvoří přílohová část, využívající dokumenty použité při Pandemii 2009/2010 z důvodu větší ilustrativnosti. Materiál byl co nejvíce zobecněn a kde jej nešlo zobecnit, zůstal nezměněn. Tyto materiály byly použity jako vzorové dokumenty. V případě jejich využití u dalších pandemií musí být aktualizovány v oblasti odborných informací a doporučení spolu s používanou terminologií v souladu s příslušnými právními předpisy (Pandemický plán rezortu zdravotnictví, 2012).

2.2.3 Pandemický plán kraje

Jde o operační plán, který je využíván v případě pandemie chřipky na území kraje. Pandemické plány kraje (dále jen „PPK“) vychází z Pandemického plánu ČR. PPK řeší problematiku pandemie chřipky na jednotlivých krajích a je v souladu s požadavky WHO a EU a jsou zde zohledněny i aspekty Sdělení Komise Radě EU, Evropského parlamentu, Evropského hospodářského a sociálního výboru a Výboru regionů.Cílem těchto plánů je co nejvíce snížit ekonomické, sociální a zdravotnické následky v případě vzniku chřipkové pandemie (Dvořák, 2009).

3 KRIZOVÉ ŘÍZENÍ

Krizové řízení je definováno zákonem č. 240/2000 Sb. „*Pro účely tohoto zákona se rozumí krizovým řízením souhrn řídících činností orgánů krizového řízení zaměřených na analýzu a vyhodnocení bezpečnostních rizik a plánování, organizování, realizaci a kontrolu činností prováděných v souvislosti s“*

- *„Přípravou na krizové situace a jejich řešením, nebo*
- *Ochranou kritické infrastruktury“* (Česko, 2000).

Orgány krizového řízení jsou:

- vláda,
- ministerstva a jiné ústřední správní úřady,
- Česká národní banka,
- orgány kraje a další orgány s působností na území kraje,
- orgány obce s rozšířenou působností,
- orgány obce (Česko, 2000).

Primární plánovací dokument, ve kterém jsou obsažena krizová opatření a postupy k řešení krizových situací se nazývá **krizový plán**. Jeho smyslem je utvořit podmínky pro zabezpečení připravenosti na krizové situace a jejich řešení pro orgány krizového řízení a další vybrané subjekty (Krizové plánování, c2022).

Krizové plány jsou tvořeny:

- ministerstvy a jinými ústředními orgány,
- Českou národní bankou,
- ostatními státními orgány, kterým krizový zákon dává za povinnost vytvářet tyto plány,
- kraji,
- obcemi s rozšířenou působností.

Plán se dělí na část základní, operativní a pomocnou (Krizové plánování, c2022).

Podnikající fyzické osoby a právnické osoby vytváří **plán krizové připravenosti.** Tyto osoby mají za úkol zabezpečit plnění opatření plynoucích z krizového plánu. Plán obsahuje přípravu určitých podnikajících fyzických osob nebo právnických osob k řešení krizové situace. Je složen ze tří částí, a to ze základní, operativní a pomocné (Krizové plánování, c2022).

Plán krizové připravenosti subjektu kritické infrastruktury je vytvářen subjekty kritické infrastruktury (dále jen „KI“). Děje se tomu tak za účelem ochrany prvku KI. Jsou zde ztotožněny hrozby, které mohou ohrozit funkci prvku KI a jsou zde také předepsána opatření pro ochranu KI. Plán krizové připravenosti subjektu KI je složen z části základní, operativní a pomocné (Krizové plánování, c2022).

Dokument popisující činnosti i opatření vedoucí k odstranění nebo ke snížení dopadů mimořádné události nebo havárie se nazývá **havarijní plán**. Máme několik typů havarijních plánů. **Havarijní plán kraje** je vytvářen pro řešení mimořádných událostí. Tyto události si žádají vyhlášení třetího stupně či zvláštního stupně poplachu podle poplachového plánu. V tomto případě zpracovává plány Hasičský záchranný sbor kraje (Havarijní plánování, c2022).

Při zpracování této dokumentace vychází z:

- analýzy vzniku mimořádné události (dále jen „MU“) a tím plynoucího nebezpečí hrozící území kraje,
- informací, které byly získány od právnických a fyzických podnikajících osob,
- informací, získaných od dotčených správních úřadů, obecních úřadů a složkami integrovaného záchranného systému (dále jen „IZS“) (Dvořáková, 2019).

Tento dokument pomáhají zpracovávat i další subjekty a složky IZS. Je schvalován hejtmanem, a to po předchozím projednáním bezpečnostní radou kraje. Jsou vytvořena minimálně dvě vyhotovení. V plánu je obsažen popis území kraje. Je zde uvedena analýza rizik vzniku MU. Poskytuje informace týkající se sil a prostředků, které lze využít k provádění záchranných a likvidačních prací. Uvádí i jakým způsobem bude zajištěna ochrana obyvatelstva v kraji. Plán je tvořen částí informační, operativní a plány konkrétních činností (Dvořáková, 2019).

Vnější havarijní plán je vytvářen pro jaderné zařízení nebo pracoviště IV. kategorie i pro objekty a zařízení, které svým charakterem mohou způsobit závažnou havárii zapříčiněnou nebezpečnými chemickými přípravky a látkami (Havarijní plánování, c2022).

Vnitřní havarijní plán je tvořen ve spolupráci se zaměstnanci provozovatele a určuje opatření v rámci objektu v případě započetí závažné havárie. Tato opatření vedou ke snížení dopadů havárie (Dvořáková, 2019).

Je zpracováván:

- těmi provozovateli objektů a zařízení, kde může vzniknout riziko závažné havárie a jsou řazeni do skupiny B, podle zákona o prevenci závažných havárií a jejich povinností je zpracovat bezpečnostní zprávu,
- provozovateli jaderných zařízení či pracovišť kategorie IV. (Havarijní plánování, c2022).

4 KYBERNETICKÁ BEZPEČNOST

„Je stav, kdy jsou na nejnižší míru eliminovány hrozby pro ČR působící z kybernetického prostoru“ (Feix a Procházka, 2017*).*

Kybernetická bezpečnost se stala jednou z mnoha důležitých částí současného světa. V digitálním prostředí se v dnešní době pohybuje velká spousta obyvatelstva. Z tohoto důvodu je potřeba si své cenné a citlivé informace chránit prostřednictvím kybernetické bezpečnosti před poškozením či krádeží (Kumar a Kaur, 2022).

S tím, jak se současný svět vyvíjí, rostou i hrozby kybernetické či kybernetické útoky. Určité úrovně bezpečnosti lze pak dosáhnout po přijmutí vhodných prostředků pomocí vícevrstvé ochrany prostřednictvím kybernetické bezpečnosti. Kybernetická bezpečnost představuje určitý proces, který je využit při kritické ochraně systémů před ztrátou, odcizením, zneužitím nebo poškozením dat (Kumar a Kaur, 2022).

4.1 Kybernetický útok

V posledních deseti letech se kybernetické útoky staly docela běžnou situací. Oběťmi těchto útoků bývají jak fyzické osoby, tak i firmy a státní instituce nevyjímaje. Může jít o útoky neškodné, které svým chováním obtěžují uživatele, avšak neohrožují svými vlastnostmi citlivá data (Siroli, 2006).

Závažnějšími jsou pak krádeže dat, vniknutí do emailů či odcizení identity. Velké škody pak mohou napáchat útoky, které vedou k zablokování funkčnosti systému. Tyto útoky pak mohou mít velký negativní dopad pro firmy, které svou aktivitu realizují v rámci elektronické komunikace. Závažným problémem také může být kybernetická špionáž státní správy nebo takové útoky, které by měly negativní dopad na kritickou infrastrukturu státu (Siroli, 2006).

Rostoucí zabezpečení a poučení uživatelů má za následek snížení nákladů na jednotlivý incident. Avšak z důvodu vzrůstajícího množství incidentů zároveň vzrůstá i souhrn celkových nákladů. Stejně tak jako narůstají drobné incidenty, narůstají i incidenty s větším i velkým rozsahem. Tyto útoky jsou pak zahrnuty v kontextu krizového řízení. Kybernetickým útokem se tímto myslí záměrné zapříčinění události, která způsobí narušení normální funkce systému. Může jít o narušení celistvosti dat a oslabení spolehlivosti systému, které následně zapříčiňuje jeho nedostupnost a plnou nefunkčnost (Mareš, Rektořík a Šelešovský, 2013).

4.2 Útoky na české nemocnice

Sítě zdravotnických zařízení v ČR a jejich zabezpečení častou nejsou prioritou. Není zde dostatek kvalifikovaného personálu starajícího se o techniku a financování tohoto sektoru je poddimenzováno. I kvůli těmto problémům jsme si v nedávné době mohli všimnout několika velkých útoků mířených proti veřejné správě a nemocnicím. Tyto instituce kvalitou zabezpečení sítí značně zaostávají za komerčním sektorem. Náklady na zabezpečení jsou však v převážné většině nižší než možné škody zapříčiněné útokem.

V případě úspěšného útoku může být paralyzována činnost celé nemocnice. Není možný přístup k rezervačnímu systému, nelze dohledat data o pacientech a v některých případech může být omezeno ovládání zdravotnických přístrojů. Mohou být odcizeny zdravotnické záznamy o pacientech či záznamy z výzkumů. Pokusy o krádež záznamů z výzkumu byly pozorovány například u vývoje vakcín proti onemocnění Covid–19. V neposlední řadě může dopad kybernetického útoku zapříčinit nedůvěryhodnost kritické infrastruktury z pohledu obyvatelstva. Ti do ní totiž vkládají své nejcitlivější informace. Útoky na nemocnice jsou buď cílené nebo jsou terčem hromadného útoku. Cílem je pak ve většině případů finanční obohacení útočníka. Občas se také může stát, že cílem útočníka je pouze snaha vytvořit škodu dané instituci (Nemocnice pod náporem…, 2021).

Velmi častým typem útoku na zdravotnická zařízení je phishingový útok. Tímto útokem se útočník snaží vytvářet dojem důvěryhodné autority jehož cílem je získání citlivých dat od oběti. Často se jedná o podvodné phishingové e-maily. Nemocnice po celé ČR se s těmito útoky setkávají i několikrát do měsíce (Pika, 2022).

II. PRAKTICKÁ ČÁST

5 FAKULTNÍ NEMOCNICE BRNO

Jedná se o druhou největší nemocnici v České republice. Současně jde o nemocnici, která má evropský význam. Svou specializovanou a superspecializovanou péči nabízí pacientům všech věkových skupin. Tuto péči nabízí ve všech medicínských odvětvích za pomocí poznatků ze současné lékařské vědy (Fakultní nemocnice Brno, 2017).

Nemocnice je financována primárně z příjmů, které jsou získávány z poskytnutí léčebné péče od zdravotních pojišťoven. Díky modernímu vybavení nemocnice, vzdělaným odborníkům, spolupráci s Masarykovou univerzitou v Brně a jiným faktorům, patří nemocnice mezi špičková zdravotnická zařízení v českém zdravotnictví. Ministerstvo zdravotnictví ČR je zřizovatelem Fakultní nemocnice Brno (dále jen „FN Brno“) (Fakultní nemocnice Brno, 2017).

V roce 2021 bylo pod FN Brno zaměstnáno 5 749 lidí ze zdravotnického i nezdravotnického sektoru. Bez specializované způsobilosti zde pracovalo 31, 86 % lékařů a se specializovanou způsobilostí 68, 14 % lékařů. Číslo týkající se počtu provedených ambulantních vyšetření se vyšplhalo až na 1 660 205 za rok 2021. Nemocnice roku 2018 disponovala lůžky v počtu 1 890 kusů. K roku 2021 se toto číslo snížilo na 1 861 kusů. Počet operací se zastavil na čísle 44 096. Dále se zde narodilo za rok 2021 6 221 dětí (Výroční zpráva 2021, 2022).

Náklady nemocnice za rok 2022 byly celkem 12 685 985 144, 66 Kč. Rozpočet, který byl schválen na rok 2023 představuje částku 13 691 401 946, 56 Kč. Na druhou stranu výnosy nemocnice za rok 2022 činily 12 733 943 259, 33 Kč (Rozpočet nákladů a výnosů 2023 až 2025, 2023).

Nemocnice se skládá ze tří pracovišť, kterými jsou:

- Pracoviště medicíny dospělého věku, které se nachází v Brně–Bohunicích, ulice Jihlavská.
- Pracoviště dětské medicíny, které je dislokováno v Černých polích a nese název Dětská nemocnice Fakultní nemocnice Brno.
- Pracoviště reprodukční medicíny ležící na Obilním trhu (Fakultní nemocnice Brno, 2017).

5.1 Areál Bohunice

Městský chorobinec z roku 1934 tvoří základ bohunické nemocnice. Požadavek na vybudování nemocnice pro město Brno se po druhé světové válce stupňoval. Rozšiřování nemocnice začalo až od roku 1969. Na konci roku 1989 byl slavnostně otevřen tzv. Lůžkový trakt, jenž je dominantou tohoto areálu. Komplex centrálních operačních sálů byl vybudován roku 1992, a stal se tak největším na Moravě (Fakultní nemocnice Brno, 2017). Roku 1999 byla nemocnice rozšířena o Kliniku ústní, čelistní a obličejové chirurgie. Téhož roku byla vybudována i Ústavní lékárna (Historie FN Brno).

Pro kraje jako je Jihomoravský, část Zlínského a Vysočinu, funguje nemocnice v Bohunicích jako Traumacentrum pro dospělé od roku 2008. Traumacentrum FN Brno je největší v ČR. Posledním dílem skládačky při tvorbě tohoto Traumacentra byl v roce 2010 vznik Spinální jednotky a druhé Jednotky intenzivní péče Ortopedické kliniky. Bohunický areál disponuje mimo jiné dvěma heliporty, kde je možný příjem letecky transportovaných pacientů. Provoz prvního heliportu byl zahájen v roce 2005 na střeše pavilonu I1. Druhý heliport byl zprovozněn roku 2015 (Fakultní nemocnice Brno, 2017; Historie FN Brno).

Obrázek 1 Areál FN Brno Bohunice (FN Brno)

5.2 Dětská nemocnice FN Brno

V Černých Polích byl zahájen provoz nemocnice Františka Josefa I. roku 1899. K tomuto roku se váže vznik Dětské nemocnice. Rekonstrukci a dostavbu nemocnice rozhodl po druhé světové válce Zemský národní výbor. Od roku 1957 se Dětská nemocnice stává Fakultní dětskou nemocnicí (Historie FN Brno).

Modernizace a rekonstrukce dětské nemocnice započala roku 1993. Proběhla výstavba nových operačních sálů a rekonstrukce objektů z roku 1953. Pracoviště umístěné mimo areál Dětské nemocnice se mohla začlenit do areálu po rekonstrukci zahájené v roce 1996 (Historie FN Brno). Na léčbu solidních nádorů dětí napříč Moravou se specializuje Klinika dětské onkologie vytvořena roku 1998. Hlavě tato klinika má v současné době velmi významné postavení (Fakultní nemocnice Brno, 2017; Historie FN Brno).

Jedno ze dvou vysoce specializovaných dětských traumacenter v ČR se od roku 2000 nachází právě v Dětské nemocnici. Nová jednotka intenzivní péče-transplantační jednotka zde byla vytvořena v roce 2006. Při Klinice dětské chirurgie, ortopedie a traumatologie se v roce 2009 otevřela doposud jediná Laboratoř chůze v ČR (Historie FN Brno).

Obrázek 2 Dětská nemocnice FN Brno (FN Brno)

5.3 Porodnice FN Brno–Obilní trh 11

Již roku 1888 se začíná psát historie Porodnice na Obilním trhu. V tomto období zde totiž vznikla tzv. Zemská porodnice. Porodnice se po vzniku Československé republiky a Masarykovy univerzity stala místem výuky porodnictví a gynekologie. V tomto období zde vznikla Gynekologicko-porodnická klinika Lékařské fakulty Masarykovy univerzity, jenž zde stále působí (Fakultní nemocnice Brno, 2017).

V 50. letech 20. století byla významná spolupráce porodnicko-pediatrická a byla rozvíjena neonatologie. Toto pracoviště se stalo průkopníkem na poli asistované reprodukce ve druhé polovině 80. let 20. století. Pacientkám a rodičkám je v současné době nabízena komplexní péče napříč spektrem svého oboru (Fakultní nemocnice Brno, 2017).

Gynekologicko-porodnická klinika Lékařské fakulty Masarykovy univerzity a FN Brno se řadí mezi největší porodnická pracoviště ve střední Evropě. V průběhu jednoho roku zde proběhne více než šest tisíc porodů. Nachází se na dvou místech, a to na Obilním trhu a v areálu FN Brno v Bohunicích (Fakultní nemocnice Brno, 2017).

Je plánováno sjednocení obou pracovišť do areálu Bohunice a vybudování supermoderní porodnice. Vybudování nové porodnice je jedním z hlavních projektů Ministerstva zdravotnictví ČR a její rozpočet by měl být 1, 9 miliardy Kč (Fakultní nemocnice Brno, 2017).

Obrázek 3 Porodnice FN Brno–Obilní trh 11(iDNES, 2009)

6 VYBRANÉ KYBERNETICKÉ HROZBY A JEJICH STATISTIKA

Autor v této části zdůvodňuje výběr svých kybernetických hrozeb. Vybranými hrozbami jsou ransomware a phishing. Tyto kybernetické hrozby jsou jedny z nejvíce používaných a nebezpečných po celém světě. Česká republika je tímto druhem kybernetické hrozby rovněž ohrožena. Mohou zapříčinit velké komplikace ve státním i soukromém sektoru. Útočník za jejich pomoci může například odcizit data z organizací a za vrácení odcizených dat požadovat výkupné, nebo může získat údaje k platebním kartám či bankovním účtům obětí.

Autor se hlavně zaměřuje na kybernetický útok phishingem, protože jde o nejčastější typ kybernetického útoku v posledních letech. A útok ransomwarem hlavně proto, že v posledních letech tento typ útoku byl veden proti několika českým zdravotnickým institucím. Velmi medializované byly například útoky na nemocnici v Benešově, psychiatrickou nemocnici v Kosmonosech a FN Brno. Důvod výběru těchto typů útoků je dále podložen statistikami zahraničními i statistikou českou, a to zpracovanou Národním úřadem pro kybernetickou a informační bezpečnost.

6.1 Statistika kybernetických útoků ve světě

Podle AAG IT (2023) je nejčastější kybernetickou hrozbou, které jednotlivci a podniky čelí, phishing. Za rok 2020 narostlo množství malwarových útoků oproti roku 2019 o 358 %. O dalších 125 % se útoky zvýšily v roce 2021 Za první pololetí roku 2022 bylo napříč celým světem zaznamenáno asi 236, 1 milionů útoků ransomwaru (The Latest 2023 Cyber Crime Statistics…, 2023).

Velký vliv měla i invaze Ruska na Ukrajinu. Od té doby se ruské phishingové útoky směřující proti e-mailovým adresám v evropských a amerických podnicích zvýšily osminásobně (The Latest 2023 Cyber Crime Statistics…, 2023).

Za rok 2021 mělo být phishingem poškozeno 323 927 uživatelů internetu. Polovina uživatelů, která zaznamenala únik dat, byla tedy postihnuta právě phishingovým útokem. Jedna miliarda e-mailů, která byla zaznamenána v roce 2021, ovlivnila jednoho z pěti uživatelů internetu. Toto číslo z části ukazuje nadále trvající prevalenci phishingových útoků. Avšak oproti ostatním útokům byl phishing nejméně ztrátovým pro oběti (The Latest 2023 Cyber Crime Statistics…, 2023).

Covid–19 značně ovlivnil počet obětí zasažených kybernetickým útokem za hodinu. Podle statistik byl za rok 2019 počet těchto obětí 53 za hodinu. V roce 2020 již počet obětí za hodinu stoupl na 90 (The Latest 2023 Cyber Crime Statistics…, 2023).

V roce 2021 byly zjištěny některé rozdíly v typech útoků používaných při pronikání do organizací. V Asii byl ransomware druhým nejčastějším typem tohoto útoku s 11 % z celkového počtu. V Evropě tento útok představoval 26 % z celkového počtu útoků a byl tedy nejčastěji používaným útokem (The Latest 2023 Cyber Crime Statistics…, 2023).

Severní Amerika byla rovněž nejčastěji zasažena ransomwarem s 30 % z celkového počtu útoků. I v Latinské Americe je na prvním místě ransomware s podílem 29 % (The Latest 2023 Cyber Crime Statistics…, 2023).

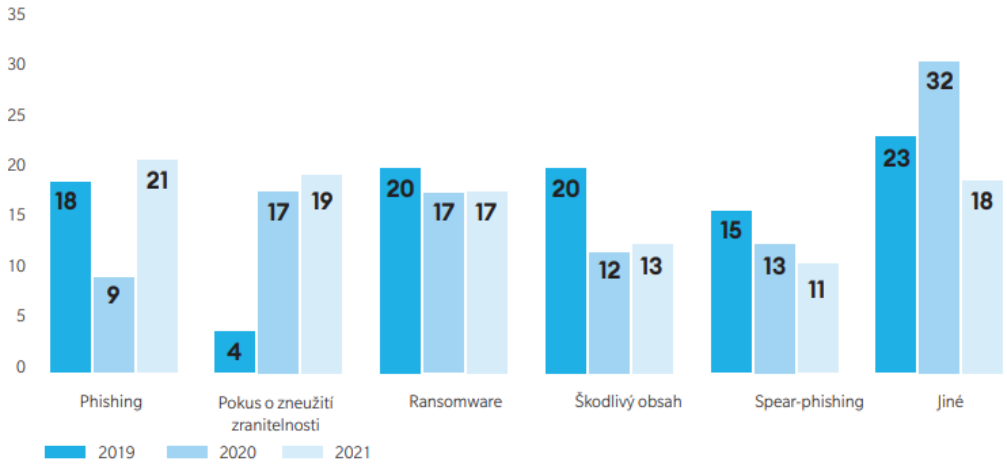
Celkem 78 % indických organizací v roce 2021 zaznamenalo útok ransomwarem. Z toho 80 % těchto útoků vedlo k zašifrování dat. V Malajsii roku 2021 bylo terčem ransomwarových útoků 79 % malajských organizací. Z toho 64 % útoků zapříčinilo šifrování dat. Za první polovinu roku pandemie Covid–19 obdrželo 34 % Kanaďanů minimálně jeden phishingový e-mail. U britských podniků v roce 2022 byl nejčastěji identifikovaným útokem phishing. Ten tvořil 83 % ze všech zaznamenaných útoků. Z ruských adres bylo v roce 2022 odesláno za jediný den přes osm miliard phishingových e-mailů (The Latest 2023 Cyber Crime Statistics…, 2023).

6.2 Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020 a 2021

Podle Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB) byly nejčastějšími typy útoků za rok 2020 spam, phishing a scanning. Za rok 2021 to byly útoky typu phishing, podvodné e-maily a skenování vnější sítě (Zpráva o stavu kybernetické bezpečnosti ČR za rok 2021, 2022; Zpráva o stavu kybernetické bezpečnosti ČR za rok 2020, 2021).

Obrázek 4 Kategorie nejčastějších typů kybernetických útoků v letech 2019–2021 v % (NÚKIB, 2022)

Do nejzávažnějších hrozeb patří pro kybernetickou bezpečnost ČR kybernetická kriminalita. V roce 2020 se nejvíce odrážela v ransomwarových útocích, které byly cíleny na sektor zdravotnictví. Stejně tak i v roce 2021 se mezi nejzávažnější útoky stále řadil ransomware, společně s phishingem nebo spear–phishingem a pokusy o zneužití zranitelností. (Zpráva o stavu kybernetické bezpečnosti ČR za rok 2021, 2022; Zpráva o stavu kybernetické bezpečnosti ČR za rok 2020, 2021).



Obrázek 5 Kategorie nejzávažnějších typů kybernetických útoků v letech 2019–2021 v % (NÚKIB, 2022)

Za rok 2020 výrazně narostl trend cílených vyděračských útoků po celém světě. Z množství vyděračských útoků, které řešil NÚKIB a z jiných dostupných zdrojů plyne, že trend nárůstu těchto útoků postihl v roce 2020 i ČR. Celkem 28 % respondentů ve zprávě uvádí, že v roce 2020 zaznamenalo útok ransomwarem nebo pokus o něj (Zpráva o stavu kybernetické bezpečnosti ČR za rok 2020, 2021).

V porovnání s celosvětovým růstem vyděračských útoků mohou být nižší počty zachycení těchto útoků v ČR zapříčiněna větším zájmem operátorů ransomwaru na oblast západní Evropy, USA a Blízkého východu. Pravděpodobnost na zaplacení výkupného výměnou za odcizená data je totiž v těchto oblastech vyšší. To je zapříčiněno tím, že organizace často mohou využít finančních náhrad z pojištění proti vyděračským útokům. V ČR pojišťovny nechtějí uhradit škody způsobené ransomwarovým útokem a platbu výkupného odmítají i z etických důvodů. I nadále je však velká pravděpodobnost útoků na státní instituce, protože zde existuje vyšší šance na zaplacení výkupného (Zpráva o stavu kybernetické bezpečnosti ČR za rok 2020, 2021).

Za rok 2021 se až 90 % respondentů setkalo s phishingovými e-maily. Spear-phishingové e-maily postihly 47 % respondentů a podvodné e-maily zaznamenalo 84 % respondentů. Phishing je jedním z nejčastěji frekventovaných vektorů útoků. S tím je spojena i pravidelnost těchto útoků objevujících se v incidentech, které jsou hlášeny NÚKIB. Během jednoho roku NÚKIB totiž nezaregistroval phishingové a jim podobné kampaně jen ve třech měsících (Zpráva o stavu kybernetické bezpečnosti ČR za rok 2021, 2022).

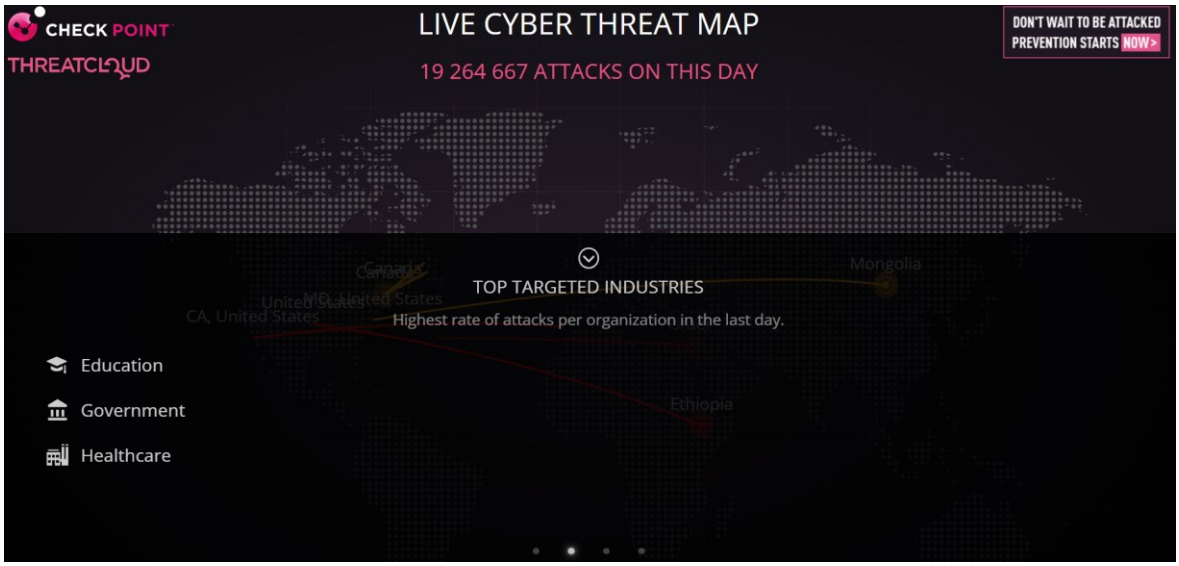
6.3 ThreatCloud World Cyber Threat Map

Tato mapa od Check Pointu umí zobrazit všechny kybernetické útoky zaznamenané bránami Check Point napříč celým světem v reálném čase. Ukazuje, jakým způsobem a kde právě probíhají kybernetické útoky. Mapa pracuje s daty, které jsou získávány z největší celosvětové sítě pro spolupráci při boji s kyberzločinem, Check Point ThreatCloud (Probíhající kyberútoky po celém světě…, 2015; Check Point představil světovou mapu…, 2015).

V databázi je obsaženo více než 250 milionů adres analyzovaných při vyhledávání botů. Přes 11 milionů malwarových signatur a více než 5, 5 milionů infikovaných webových stránek. Každý den také rozpozná miliony malwarových typů (Probíhající kyberútoky po celém světě…, 2015; Check Point představil světovou mapu…, 2015).

Na mapě je možno vidět nejdůležitější denní statistiky. Zobrazuje 10 zemí, ze kterých jsou nejčastěji útoky vysílány a 10 zemí, na které jsou útoky cíleny. Ukazuje, o jaký typ útoku se jedná a jsou zde ke spatření i počty útoků, které se za daný den odehrály. K dispozici jsou i týdenní a měsíční statistiky o infekcích a nejvíce běžné útoky individuálně pro každou zemi zvlášť (Probíhající kyberútoky po celém světě…, 2015; Check Point představil světovou mapu…, 2015).

Marketingová ředitelka společnosti Check Point Software Technologies, Marie Hattar řekla: *„Pro organizace může být těžké pochopit rychlost a globální rozměr kybernetických útoků. Chtěli jsme vytvořit nástroj, který pomůže organizacím pochopit, jak rychle se mění oblast hrozeb, aby mohly podniknout kroky k posílení bezpečnosti a lepší ochraně před útoky.“* (Probíhající kyberútoky po celém světě…, 2015; Check Point představil světovou mapu…, 2015).

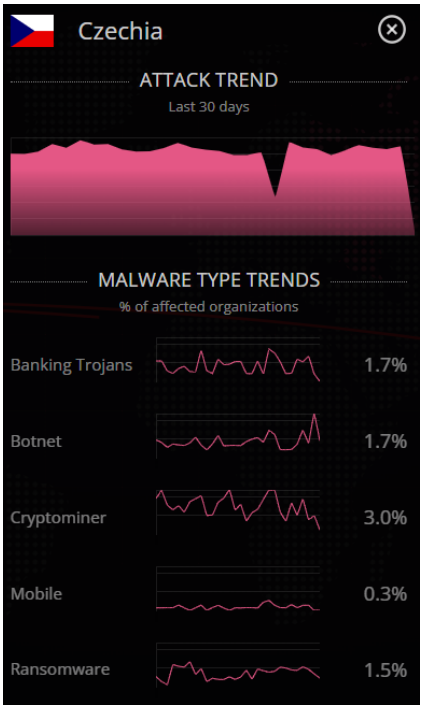


Obrázek 6 Nejčastěji cílená odvětví (Check Point Software Technologies, 2023)

Na obrázku č. 6 je možné vidět mapu Live Cyber Threat od společnosti Check Point Software Technologies ze dne 14. 4. 2023. Kde se po vybrání požadovaného sektoru zobrazí první tři odvětví, na které jsou nejčastěji cíleny kybernetické útoky. Z obrázku je patrné, že jedním ze tří nejčastěji cílených odvětví je mimo vzdělávání a vládní instituce, právě diskutované zdravotnictví, které je každým dnem vystavováno kybernetickým útokům po celém světě.

Obrázek 7 Nejčastější typy malwaru (Check Point Software Technologies, 2023)

Podle obrázku č. 7 lze vypozorovat tři nejčastější malwarové útoky. Dne 15. 4. 2023 byl phishing nejčastěji používaným malwarovým typem kybernetického útoku napříč celým světem.



Obrázek 8 Trendy typů malwaru v ČR
(Check Point Software Technologies, 2023)

Obrázek č. 8 popisuje trendy malwarových kybernetických útoků v rámci České republiky za posledních třicet dní. To znamená, že byl tento průběh zaznamenáván od 16. 3. 2023 do 15. 4. 2023. Ze všech útoků, které byly provedeny na jednotlivé organizace napříč ČR, tvořil ransomware 1,5% podíl.

7 ŘÍZENÝ ROZHOVOR S ODBORNÍKEM NA KYBERNETICKOU BEZPEČNOST

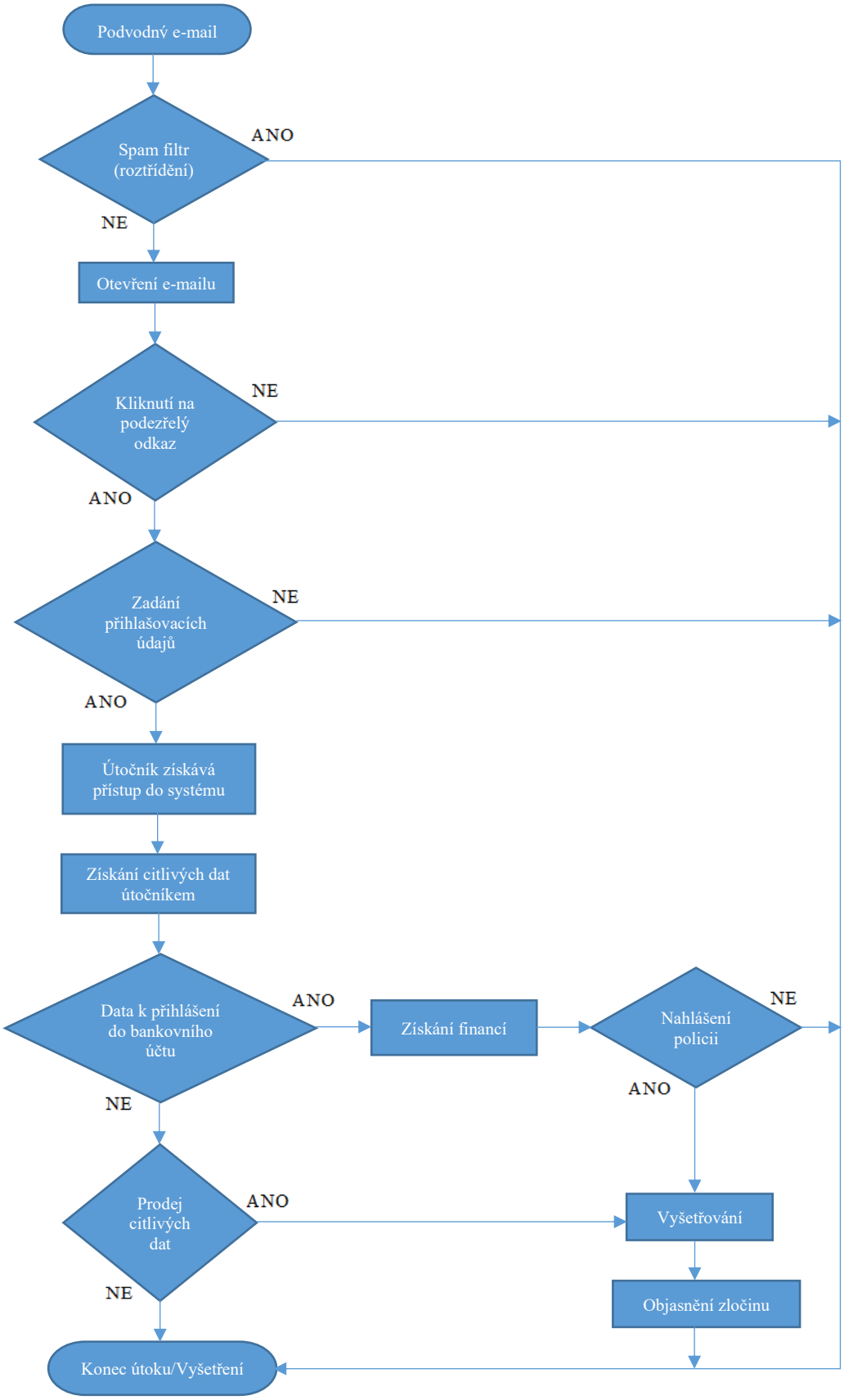
Tento rozhovor proběhl dne 8. 4. 2023 za účelem zjištění informací, potřebných pro analýzu vybraných kybernetických útoků a jejich následných dopadů, které by teoreticky mohly být na vybrané nemocniční zařízení směřovány. Rozhovor se odvíjel od předem připravených otázek a dotazníku, který autor sestavil. Některé otázky a dotazník byly následně podrobněji rozebrány odborníkem na kybernetickou bezpečnost, a to náměstkem pro informatiku. Vybrané útoky by mohly mít v některých případech pro vybrané nemocniční zařízení velmi vážné následky.

Podle slov odborníka na kybernetickou bezpečnost byly kybernetické útoky v období pandemie Covid–19 více medializované než mimo toto období. I díky tomuto faktu si může laická veřejnost myslet, že za období pandemie byly útoky mnohem více frekventovanější než mimo období pandemie Covid–19. Statistiky ukazují, že počty kybernetických útoků napříč světem se v roce 2020 prudce navýšily oproti roku 2019. Častěji objevující se články o kybernetických útocích však nemusí být automaticky přímou úměrou ke zvyšujícím se počtům kybernetických útoků.

Dalším důvodem zvyšujícího se povědomí veřejnosti o kybernetických hrozbách a útocích může být, že za období pandemie spousta lidí pracovala z domovů přes počítač a za dobu lockdownu byla v ČR spousta činností omezena. To v praxi znamenalo přesun obyvatel z reálného světa do světa virtuálního. Jak se zvyšoval čas strávený doma u počítače, tak se zvyšovalo i povědomí o kybernetických hrozbách. Současně se i zvyšovalo riziko, že se uživatel počítače stane obětí kybernetického útoku.

Cílené hrozby typu ransomware a podobně nebyly nijak zvlášť ovlivněny, co se počtu útoků týká, pandemií Covid–19. Dle názoru odborníka na kybernetickou bezpečnost má na množství kybernetických útoků větší vliv než pandemie Covid–19, právě probíhající invaze na Ukrajině. Ruská federace totiž disponuje poměrně rozsáhlou a schopnou armádou v oblasti kybernetiky. Z tohoto důvodu představuje hrozbu v oblasti kybernetické bezpečnosti.

Níže jsou zobrazeny vývojové diagramy pro kybernetické útoky typu phishing a ransomware, které jsou zde uvedeny z důvodu lepší představy o průběhu těchto útoků.



Obrázek 9 Vývojový diagram–phishing (autor, 2023)

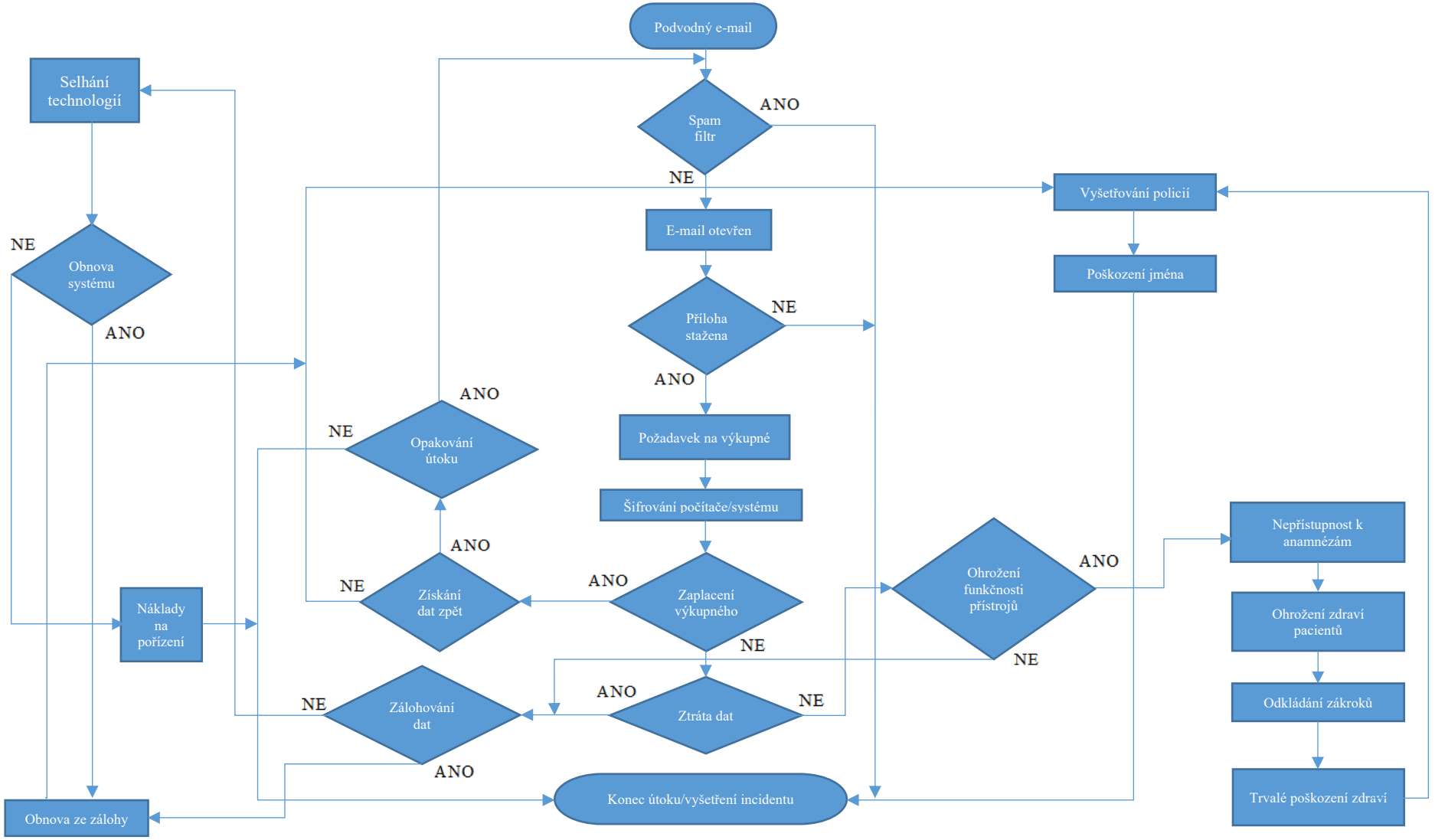
7.1 Průběh phishingu

Při útoku phishingem se jedná ve většině případů o zaslání podvodného e-mailu. Tyto e-maily jsou buď cílené na určitou osobu nebo instituci a jedná se tak o spear phishing, kde je podvodný e-mail sestaven podle dostupných informací o osobě či instituci. Phishing může také být rozesílán hromadně, a to bez určitého cíle. Tento podvodný e-mail obsahuje odkazy na falešné, avšak důvěryhodně vypadající webové stránky a nutí oběť k zadání svých osobních údajů (Phishing, c1992-2023).

V první fázi, aby mohl vůbec incident proběhnout, musí přijít do e-mailové schránky oběti falešný e-mail. Po odeslání e-mailu útočníkem, tato zpráva leží ve schránce potencionální oběti. Vzniku neštěstí může předejít spamový filtr, který může na základě pravidel filtru označit zprávu za spam. Pokud je zpráva označena jako spam, tak se po určité době takto označená pošta sama maže. Při takovémto hladkém průběhu situace je nebezpečí zažehnáno hned ze začátku a žádný problém nenastává.

Podvodný e-mail nemusí být vždy dobře rozeznatelný, a tak nemusí dojít k jeho správnému roztřídění do spamové pošty. Zde hrozí riziko, že oběť obdržený e-mail může otevřít. Samotné otevření nevyžádané pošty nepředstavuje přímé ohrožení. Problém nastává s kliknutím na odkaz či stáhnutím přílohy v této poště. Působí-li doručená pošta věrohodně a příjemce nerozezná skutečný e-mail od podvodného, tak je pravděpodobné, že klikne na přiložený odkaz. Pokud je e-mail otevřen, ale uživatel neklikne na přiložený odkaz, tak opět k přímému ohrožení uživatele nedojde. Na poslední chvíli je možné problém zažehnat nezadáním přihlašovacích údajů do falešné webové stránky.

Pokud se tak nestane, útočník získává přístup do systému a mimo jiné i přístup k datům pacientů. Jedná se o anamnézy pacientů či osobní data. Tato data mohou být dále prodána třetí osobě za finanční obnos. Zdravotnické záznamy však obsahují specifická data a jejich porozumění vyžaduje určité zdravotnické vzdělání. Útočník dále může cílit svůj útok přímo na pacienty, protože získává jejich kontaktní údaje. Prostřednictvím podvodného e-mailu lze získat i údaje do bankovních účtů, kde může dojít k odcizení peněz nebo podvodným platbám z nemocnice. Další velký problém může nastat v případě, že se útočník vydává za zdravotnickou instituci, kde může požadovat různé platby nebo informace od pacientů, organizací a podobně. Tyto činy mohou mít vážné následky pro pacienty, zaměstnance i nemocnici. Reputace nemocnice je tímto útokem ohrožena a některé škody bývají nenapravitelné.



Obrázek 10 Vývojový diagram–ransomware (autor, 2023)

7.2 Průběh ransomwaru

Počátek ransomwaru je obdobný jako u útoku phishingem. Uživateli do e-mailové pošty přichází podezřelý e-mail. Ten se opět v ideálním případě nedostane přes spam filtr. Podvodný e-mail je přesměrován do složky spam a zde je následně automaticky po několika dnech smazán. Možný bezpečnostní incident je tak již v počátcích zažehnán.

V případě, že se tato nevyžádaná pošta dostane potencionální oběti mezi ostatní doručené e-maily, nastává riziko otevření uživatelem. Samotné riziko z pouhého otevření e-mailu nehrozí. Neměly by však být stahovány přílohy, a také otevírány přiložené odkazy, které jsou součástí této pošty a jsou pravděpodobně infikované. Ransomware se totiž do zařízení nejčastěji dostává zavirovanými přílohami e-mailů, návštěvami infikovaných webů, dokonce i prostřednictvím sítě, ve které se právě šíří (Ransomware, c1992-2023).

Po otevření e-mailu a stažení přílohy uživatelem, nastává problém. Na obrazovce počítače se objeví požadavek na zaplacení výkupného. Následně se zašifruje celý počítač a v horším případě probíhá šifrování celého systému.

Zjistitelnost a schopnost šířit se internetovou sítí, má vliv na efektivitu ransomwaru. Z tohoto důvodu útok, který zasáhne pouze koncové stanice nemocnice a centrální servery zůstanou nedotčeny, bude mít výrazně omezený dopad na pacienty a fungování nemocnice. I když budou ztraceny údaje na koncových stanicích, tak samotná funkčnost nemocnice je omezena jen na dobu nezbytně nutnou pro vyčištění koncových stanic.

Pokud útok postihne celou infrastrukturu nemocnice, tak jsou dopady obrovské. Nemocnice se vrací o několik desetiletí nazpět a je ohroženo zdraví pacientů. Nelze například zpracovávat mzdy, posílat výkazy či objednat léky. Nemocnice se v tu dobu stává nefunkční.

Jestli výkupné zaplatit nebo nezaplatit, už pak závisí na poškozeném zdravotnickém zařízení. To může výkupné zaplatit a odcizená data mohou být navrácena. V lepším případě útočník odcizená data vrátí po obdržení finanční částky a útok se nebude opakovat. Na druhou stranu je i možné, že podobný nebo stejný incident se v budoucnu bude opakovat. Je tomu tak proto, že pokud útočník již jednou dostal zaplaceno, může se domnívat, že dostane zaplaceno i podruhé. Také se může stát, že poškozený požadovanou finanční částku zaplatí, ale útočník odcizená data nenavrátí. Takový případ znamená obrovské ztráty pro nemocnici.

Pokud se poškozený uživatel rozhodne výkupné nezaplatit, tak hrozí nenávratnost odcizených dat. To v konečném důsledku opět ohrožuje chod celé nemocnice z důvodu, že přichází o veškeré záznamy o pacientech, hrozí poškození výzkumu nebo ztráta účetních a obchodních dat i data zaznamenána přístroji. Tehdy je důležité zálohování dat. Jestliže jsou data zálohována, tak se mohou z této zálohy později obnovit. Horším případem je, když data zálohována nejsou. V takovém případě dochází k selhání technologií a systém je nutné znovu obnovit. Ne vždy je možné systém znovu zprovoznit. Tehdy musí poškozený vynaložit značnou finanční částku na obnovu celého systému a ztracená data opět nashromáždit.

Mimo zmíněnou ztrátu dat je také ohrožena samotná funkce přístrojů. Jejich špatná nebo žádná funkce má vliv ve zdravotnických zařízeních na přístup k anamnézám pacientů. To může zapříčinit špatnou diagnózu pacienta lékařem či nemožnost celkově určit diagnózu bez přístupu k anamnéze pacienta. Následuje odkládání operačních zákroků v důsledku nefunkčnosti některých přístrojů. Což může vést ke zhoršení zdravotního stavu některých pacientů. V extrémních případech jde o trvalé poškození zdraví, kde následky mohou být fatální z pohledu zdravotního stavu pacienta.

Celý incident by prošetřovala policie. Zvlášť pokud by se jednalo o útok s dopady na celkový chod zdravotnického zařízení, kde by měly být ohroženy životy a zdraví osob. Celková medializace takových útoků a útoky samotné, mohou negativně ovlivnit dobré jméno organizace. Tyto incidenty vzbuzují nedůvěru obyvatelstva ve státní organizace a kritickou infrastrukturu.

7.3 Dopady útoků na zdravotnické zařízení

Dopady útoků na nemocnici mohou být v některých případech méně závažné. V jiných případech mohou chod nemocnice vážně ohrozit či ohrozit životy nebo zdraví samotných pacientů. Vážnost dopadů se například odvíjí od typu útoku, rozsahu poškození systému a funkčnosti přístrojů. Dochází k šifrování pevných disků, což způsobuje nepřístupnost k datům a lékaři tak nemohou plně vykonávat svou práci bez určitého rizika. Útočník si po vstupu do systému může libovolně měnit soubory a mimo jiné odepírat přístup jiným uživatelům.

V případě požadování výkupného útočníkem může nemocnice finanční částku uhradit. Samotná úhrada částky má dopady na zdravotnické zařízení v podobě finančních ztrát, protože požadované výkupné se pohybuje ve vysokých částkách.

Pojišťovny v ČR totiž zaplacení výkupného v souvislosti s kybernetickým útokem nechtějí uhradit, jako tomu naopak bývá v jiných zemích. Tyto finanční prostředky by tak byly využity mnohem efektivnějším způsobem, kdyby k žádnému útoku nedošlo. Na druhou stranu podle některých odborníků zaplacení výkupného bývá výhodnější a levnější cestou. Je tomu tak proto, že náklady na znovuobnovení systému a nápravu škod způsobených útokem jsou často mnohem vyšší než náklady vynaložené v souvislosti se zaplacením výkupného. Podle mluvčího brněnských krajských žalobců Hynka Olmy byla pří útoku ransomwarem na FN Brno předběžná vyčíslená škoda 150 milionů korun.

Při nefunkčnosti systému nebo z důvodu zabránění dalšímu šíření škodlivého kódu se v některých případech lékaři a všechen personál musí navrátit o několik desetiletí nazpět. Nemocnice se tak rázem ocitá v době, ve které neexistují moderní technologie. Opět je třeba návrat k psacím strojům a ručně vypisované dokumentaci. Není zde možnost nahlédnutí k anamnézám pacientů a do jejich zdravotní dokumentace. Po vyšetření pacienta nelze zjištěné skutečnosti ukládat do systému. Z tohoto důvodu se doba vyšetření pacienta značně prodlužuje.

Některé zdravotnické přístroje mohou být útokem negativně ovlivněny. Jejich funkčnost je tak omezena či nemusí fungovat vůbec. To má vliv na pacienty napojené na tato zařízení. Jejich zdraví je tedy útokem vážně ohroženo a je třeba učinit takové kroky, které pacienty dostanou ze situace ohrožujících jejich životy.

Na tyto komplikace navazují další, a to spojené s odkládáním operačních zákroků. Pacienti tak musí čekat několik dní či týdnů na svůj plánovaný operační zákrok, avšak bez záruky, že k zákroku opravdu dojde. Nově akutní pacienti musí být převáženi do jiných okolních nemocnic. To má v nejhorších případech dopady v podobě trvalého poškození zdraví pacienta či smrti pacienta z důvodu převozu pacienta do jiného zdravotnického zařízení. Mimo jiné je i omezen celkový příjem pacientů poškozenou nemocnicí, což v konečném důsledku může mít opět vliv na zdraví pacientů.

Některá data nemocnice mohou být trvale ztracena. Těmi jsou informace o pacientech, různé vědecké výzkumy nebo některá administrativní a ekonomická data. V případě útoku na FN Brno roku 2020 se podařilo zachovat informace o pacientech a radiologická a laboratorní data, ale výzkumná a některé ekonomická a administrativní data byla nenávratně ztracena.

Kybernetickým útokem může být v dnešní době zasažena také správa budov. Chytré zamykání dveří může pod nátlakem útoku odemknout veškeré dveře v budově, nebo je naopak uzamknout či zapříčinit nesprávnou funkci zámků. V bezpečí před útokem nejsou ani elektrické požární signalizace, které svou špatnou funkcí způsobují zbytečnou paniku a chaos v budově, nebo při skutečném požáru nesignalizují nebezpečí. Je zde i možný dopad na detektory pohybu a detektory kouře, které zajišťují bezpečnost budovy. Při výpadku kamerového systému jsou ohroženy objekty proti neoprávněnému chování a vniknutí, kdy není možné incident na kameře zaznamenat, nebo přehrát požadovaný záznam.

Následky pro nemocnici jsou dlouhodobé a mohou trvat i v rámci několika let. Několik sítí u FN Brno bylo i po několika letech stále nevyčištěných a fungovaly odděleně od ostatních bezpečných sítí. Přes rok probíhala obnova některých dat a jiná byla definitivně ztracena.

Celý incident v neposlední řadě také poškodí nemocnici v rámci její důvěryhodnosti v očích široké veřejnosti. Veřejnost tak bude mít obavy, že jejich citlivá data nejsou dostatečně chráněna před odcizením či zneužitím neoprávněnou osobou. Z toho vyplývá poškození dobrého jména zdravotnické instituce.

7.4 Porovnání období pandemie Covid–19 a běžný stav

Dle názoru odborníka na kybernetickou bezpečnost nijak velký rozdíl mezi obdobím pandemie Covid–19 a běžným stavem není. Pandemie podle jeho slov nemá vliv na závažnost kybernetických hrozeb pro zdravotnické zařízení. Úroveň hrozeb se tedy nemění a závažnost útoků je v obou obdobích stejná. Kybernetické prostředí nemocnice není zranitelnější při situacích jako je pandemie Covid–19 v porovnání s běžným stavem. Stejně tak úroveň zabezpečení se nemění. Z tohoto důvodu by útočník musel vynaložit stejné úsilí při prolomení kybernetické ochrany nemocnice, nehledě na rozdíl v těchto obdobích.
Nárůst bezpečnostních incidentů v podobě phishingu není odborník schopen vyhodnotit. Statistiky však ukazují, že za rok 2020 se počet malwarových útoků po celém světě zvýšil o 358 % oproti roku 2019 a značná část nárůstu těchto incidentů je ovlivněna právě obdobím pandemie Covid–19. Laická veřejnost si může myslet, že dochází k nárůstu kybernetických útoků v období pandemie na základě toho, že za toto období jsou kybernetické útoky více medializovány, což nutně nemusí být důkazem pro zvyšující se počty kybernetických útoků v tomto období.

Velký problém však může nastat v případě velkého počtu pacientů s velmi těžkým průběhem onemocnění Covid–19. Nemocnice se v období pandemie plnily pacienty mající těžký průběh onemocnění a spousta z nich vyžadovala napojení na umělou plicní ventilaci. V případě, že nastane kybernetický útok, mohou být tyto ventilace ohroženy na funkčnosti. Tehdy je pacient vážně ohrožen, protože pokud přestane ventilace fungovat, je znemožněno dýchání pacienta, což je neslučitelné se životem.

Dalším problémem může být fyzický i psychický nátlak na personál nemocnice. V případě, že je některý pracovník vyčerpaný, snižuje se jeho pozornost. V tomto okamžiku je například větší pravděpodobnost přehlédnutí či nevěnování dostatečné pozornosti podvodným e-mailům, které neroztřídil spam filtr. Z důvodu vyčerpáni si nemusí pracovník všimnout jinak běžně známých ukazatelů, které jsou například typické pro phishing. Těmi mohou být špatná gramatika či špatně napsaný název domény.

Velké psychické a fyzické vytížení zaměstnanců, společně s náporem pacientů trpícím onemocněním Covid–19, může v nemocnici způsobit komplikace, které v běžném stavu nejsou časté.

8 VYHODNOCENÍ VÝSLEDKŮ A NÁVRH NA ZLEPŠENÍ

Z rozhovoru vyplývá, že kybernetické útoky a kybernetickou bezpečnost pandemie Covid–19 zdravotnická zařízení v ČR nijak zvlášť neovlivnila. Závažnost dopadů je stejná pro období pandemie i období mimo ni. Bezpečnost kybernetického prostředí se s pandemií nemění a nestává se zranitelnější. Statistiky však ukazují, že za období pandemie se množství a frekvence kybernetických útoků napříč světem v mnoha odvětvích mnohonásobně zvýšila.

Vývojový diagram phishingu ukazuje, že při úspěšném útoku může dojít k proniknutí do účtů uživatele či úniku citlivých dat. Vývojový diagram ransomwaru pak ukazuje, že při použití nejhoršího scénáře, může mít tento typ kybernetického útoku pro nemocnici i pacienty velmi vážné dopady. Nemocnice se z takového útoku vzpamatovává několik týdnů či měsíců a úplné vyčištění sítí a obnova dat trvá i několik let.

Úspěšný útok by pro FN Brno znamenal ohrožení pacientů nejen z jihomoravského kraje, ale i ze sousedních krajů, kterým FN Brno poskytuje zdravotní péči. FN Brno je druhou největší nemocnicí v ČR. Ročně je zde mimo jiné provedeno přes jeden a půl milionu ambulantních vyšetření, provedeno přes čtyřicet čtyři tisíc operačních zákroků a přes šest tisíc porodů. Nemocnice tedy disponuje velkým množstvím dat a informací. Z tohoto důvodu je zde velká pravděpodobnost, že se v i budoucnu budou opakovat další pokusy o prolomení kybernetické ochrany za účelem zisku dat či financí.

Je tedy k zamyšlení, zda nenavýšit rozpočty na kybernetickou bezpečnost zdravotnických organizací, které jsou podle některých odborníků podfinancované. Ti také tvrdí, že tyto organizace trpí výrazným nedostatkem kvalifikovaného personálu v oblasti informatiky. Obsazení těchto míst by mohlo výrazně zvýšit bezpečnost kybernetického prostoru nemocnice. Lepší finanční ohodnocení těchto pracovníků by mohlo vzbudit zájem například u zkušených odborníků pracujících v soukromém sektoru.

U většiny organizací probíhá školení v oblasti kybernetické bezpečnosti jednou ročně. Rozdělit toto školení do čtyř čtvrtletních školení by mohlo být pro zaměstnance méně vyčerpávající, naopak by zaměstnanci věnovali školení více pozornosti v případě, že by zmíněné čtvrtletní školení nebylo tak zdlouhavé.

Informační struktura nemocnic navíc funguje na zastaralých systémech. Investice do kybernetické bezpečnosti, kvalifikovaný a dobře proškolený personál je klíčem k bezpečnému informačnímu prostředí.

ZÁVĚR

Práce definovala problematiku onemocnění Covid–19. Zmiňovala druhy biologických ohrožení a pandemické plány. Popisovala, jakým způsobem je vymezeno krizové řízení a rozebrala jednotlivé krizové plány. Vymezovala pojem kybernetická bezpečnost a stručně pojednávala o kybernetických útocích na česká zdravotnická zařízení.

Bylo charakterizováno vybrané zdravotnické zařízení a stručně rozebrán jeho historický vývoj. Autor uvedl i některé další informace spojené s touto organizací pro lepší představu o velikosti nemocnice a jejích kapacitách.

Dále byly popsány důvody výběru dvou kybernetických hrozeb, které mohou zdravotnické zařízení negativně ovlivnit. Tyto důvody výběru se opírají o současné statistiky z domova i ze světa a je přiloženo i grafické znázornění pro lepší představu o počtech kybernetických incidentů za posledních několik let v ČR.

Rozebíraly se informace, zjištěné z řízeného rozhovoru, který proběhl s odborníkem na kybernetickou bezpečnost. Kybernetické útoky vybrané na základě statistických údajů se zjednodušeně analyzovaly vývojovými diagramy, které byly doplněny o slovní popis. Tyto diagramy ukazují průběh útoku od samotného počátku až po konec incidentu. Z těchto diagramů byly odvozeny dopady, které nemocniční zařízení mohou postihnout v případě, že se útočníkovi podaří úspěšně proniknout do systému instituce.

Následně proběhlo srovnání dvou období, kde autor mimo jiné vychází z informací získané z řízeného rozhovoru s odborníkem na kybernetickou bezpečnost. Jednalo se o porovnání rozdílů týkajících se vlivu kybernetických útoků na nemocniční zařízení mezi obdobími pandemie Covid–19 a běžným stavem. Srovnání mělo ukázat, zda pandemie Covid–19 měla vliv na kybernetické útoky mířené proti zdravotnickým organizacím či žádné ovlivnění pandemie nezpůsobila.

Poslední část se věnovala vyhodnocení a návrhům pro zlepšení. Shrnula veškeré poznatky zjištěné z řízeného rozhovoru, a také informace vyplývající z vývojových diagramů. Autor navrhnul některé kroky, které by mohly vést ke zlepšení kybernetické bezpečnosti zdravotnických zařízení.

SEZNAM POUŽITÉ LITERATURY

Česko, 2000. Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů. *Sbírka zákonů České republiky.* [online]. [cit. 2022-11-8]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-240.

DVOŘÁK, Pavel, 2009. Pandemický plán Kraje Vysočina. *Kraj Vysočina* [online]. [cit. 2022-11-8]. Dostupné z: https://archiv.krvysocina.cz/assets/File.ashx?id_org=450008&id_dokumenty=4069438

DVOŘÁKOVÁ, Kamila, 2019. Havarijní a krizové plánování. *HZS Jihočeského kraje, Územní odbor České Budějovice* [online]. České Budějovice: HZS Jihočeského kraje [cit. 2022-11-04]. Dostupné z: https://www.cbudejovice.cz/sites/default/files/obsah/Odbory/KPKZ/skoleni/havarijni_a_krizove_planovani.pdf

Fakultní nemocnice Brno, 2017. *Fakultní nemocnice Brno* [online]. Brno: FN Brno [cit. 2023-04-01]. Dostupné z: https://www.fnbrno.cz/prezentacni-publikace-o-fn-brno/f3642

FEIX, Miroslav a Dalibor PROCHÁZKA, 2017. Aktuální úkoly kybernetické obrany rezortu Ministerstva obrany. *Vojenské rozhledy* [online]. Univerzita obrany [cit. 2023-02-24]. Dostupné z: https://www.researchgate.net/publication/319626738_Recent_Objectives_of_Cyber_Defence_in_the_Department_of_Defence/fulltext/59b684c1458515c212b268f2/Recent-Objectives-of-Cyber-Defence-in-the-Department-of-Defence.pdf

HARNACH, Richard, 1960. *Nakažlivé nemoci hospodářských zvířat*: uče. pro vet. Fak. Vys. škol. zeměd. 2. přeprac. A dopln. Vyd. Paha: SZN, s. 413

Havarijní plánování, c2022. *HZS ČR* [online]. Praha: Generální ředitelství Hasičského záchranného sboru ČR [cit. 2022-11-04]. Dostupné z: https://www.hzscr.cz/clanek/krizove-rizeni-a-cnp-havarijni-planovani-havarijni-planovani.aspx?q=Y2hudW09MQ%3d%3d

Historie FN Brno. *Fakultní nemocnice Brno* [online]. Brno: FN Brno [cit. 2023-04-02]. Dostupné z: https://www.fnbrno.cz/historie-fn-brno/t5760

HONZÁK, Radkin et al., 2020. *Doba koronavirová*. Praha: Zeď, 305 s. ISBN 9788090767447.

HU, Ben et al., 2020. Characteristics of SARS-CoV-2 and COVID-19. *Nature Reviews Microbiology* [online]. Springer Nature [cit. 2023-02-24]. Dostupné z: https://www.nature.com/articles/s41579-020-00459-7

HUANG, Boxuan et al., 2020. Characteristics of the Coronavirus Disease 2019 and related Therapeutic Options. *National Library of Medicine* [online]. National Library of Medicine [cit. 2023-02-24]. Dostupné z: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7311344/

Check Point představil světovou mapu kyberhrozeb v reálném čase, 2015. *E15* [online]. Praha: Czech News Center [cit. 2023-04-15]. Dostupné z: https://www.e15.cz/byznys/technologie-a-media/check-point-predstavil-svetovou-mapu-kyberhrozeb-v-realnem-case-1191418

JIANG, Fang et al., 2020. Review of the Clinical Characteristics of Coronavirus Disease 2019 (COVID-19). *Springer Link* [online]. Springer Nature [cit. 2023-02-24]. Dostupné z: https://doi.org/10.1007/s11606-020-05762-w

Krizové plánování, c2022. *HZS ČR* [online]. Praha: Generální ředitelství Hasičského záchranného sboru ČR [cit. 2022-11-03]. Dostupné z: https://www.hzscr.cz/clanek/krizove-rizeni-a-cnp-krizove-planovani-krizove-planovani.aspx

KUMAR, Tanya and Satveer KAUR, 2022. Cyber Security in Businesses: Challenges and Recovery Modes. *IEEE Xplore* [online]. Yemen: IEEE [cit. 2023-02-24]. Dostupné z: https://ieeexplore.ieee.org/document/9935439

MÁJEK, Ondřej. 2020. Význam a výpočet reprodukčního čísla R. *Ministerstvo zdravotnictví České republiky* [online]. Praha: Ministerstvo zdravotnictví České republiky, [cit. 2022-10-29]. Dostupné z: https://onemocneni-aktualne.mzcr.cz/doc/2020-03-27-cislo-R.pdf

MAREŠ, Miroslav, Jaroslav REKTOŘÍK a Jan ŠELEŠOVSKÝ, 2013. *Krizový management: případové bezpečnostní studie*. Praha: Ekopress, 237 s. ISBN 9788086929927.

NAQVI, Ahmad A. T. et al., 2020. Insights into SARS-CoV-2 genome, structure, evolution, pathogenesis and therapies: Structural genomics approach. *Science Direct* [online]. Elsevier [cit. 2023-02-24]. Dostupné z: https://www.sciencedirect.com/science/article/pii/S092544392030226X?via%3Dihub#t0005

Nemocnice pod náporem hackerů: Jak proběhly nejznámější kyberútoky na české nemocnice?, 2021. *Avast* [online]. Praha: Avast Software [cit. 2022-12-22]. Dostupné z: https://blog.avast.com/cs/nemocnice-pod-naporem-hackeru-jak-probihaji-kyberutoky-na-ceske-nemocnice

Onemocnění aktuálně, 2023. *COVID-19: Přehled aktuální situace v ČR* [online]. Praha: Web studio [cit. 2023-01-07]. Dostupné z: https://onemocneni-aktualne.mzcr.cz/covid-19

Pandemické plány, c2016–2022. *Pandemie* [online]. pandemie.cz [cit. 2022-11-08]. Dostupné z: https://www.pandemie.cz/pandemicke-plany

Pandemický plán České republiky, 2011. *Ministerstvo zdravotnictví* [online]. Praha: Ministerstvo zdravotnictví ČR [cit. 2022-11-8]. Dostupné z: https://www.mzcr.cz/wp-content/uploads/wepub/5520/14546/Pandemick%C3%BD%20pl%C3%A1n%20%C4%8CR.pdf

Pandemický plán rezortu zdravotnictví, 2012. *Ministerstvo zdravotnictví* [online]. Praha: Ministerstvo zdravotnictví ČR [cit. 2022-11-8]. Dostupné z: Pandemický plán rezortu zdravotnictví – Ministerstvo zdravotnictví (mzcr.cz)

Pandemie vs epidemie, c2016–2022. *Pandemie* [online]. pandemie.cz [cit. 2022-11-01]. Dostupné z: https://www.pandemie.cz/pandemie-vs-epidemie

PEŠAN, Michal, 2010. Systém krizového řízení v oblasti dopravy. *Ministerstvo vnitra generální ředitelství Hasičského záchranného sboru ČR* [online]. ISBN 978-80-86640-57-0. [cit. 2022-11-04]. Dostupné z: https://www.hzscr.cz/soubor/vzdelavani-v-krizovem-rizeni-moduly-modul-f-pdf.aspx

Phishing, c1992-2023. *Eset* [online]. eset [cit. 2023-04-15]. Dostupné z: https://www.eset.com/cz/phishing/#

PIKA, Tomáš, 2022. Phishing, ransomware nebo skenování systému. Nemocnice stále čelí kybernetickým útokům. *iRozhlas* [online]. Praha: Český rozhlas [cit. 2022-12-22]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/kyberneticka-bezpecnost-nemocnice-zdravotnicka-zarizeni_2205010600_pik

Probíhající kyberútoky po celém světě v reálném čase a online na mapě od Check Pointu, 2015. *Security magazím* [online]. Praha: Security media [cit. 2023-04-15]. Dostupné z: https://www.securitymagazin.cz/security/probihajici-kyberutoky-po-celem-svete-v-realnem-case-a-online-na-mape-od-check-pointu-1404045438.html

Ransomware, c1992-2023. *Eset* [online]. eset [cit. 2023-04-21]. Dostupné z: https://www.eset.com/cz/ransomware/

REHMAN, Saif et al., 2020. Evolutionary Trajectory for the Emergence of Novel Coronavirus SARS-CoV-2. *MDPI* [online]. MDPI [cit. 2023-02-24]. Dostupné z: https://www.mdpi.com/2076-0817/9/3/240

Rozpočet nákladů a výnosů 2023 až 2025, 2023. *Fakultní nemocnice Brno* [online]. Brno: FN Brno [cit. 2023-04-01]. Dostupné z: https://www.fnbrno.cz/rozpocet-nakladu-a-vynosu-2023-az-2025/f5701

SIROLI, Gian P., 2006. *Strategic Information Warfare: An Introduction*. In Halpin, E., Trevorrow, P., Webb, D., Wright, S. Cyberwar, Netwar and the Revolution in Military Affairs. New York: Palgrave Macmillan, s. 32–48. ISBN 1-4039-8717-3.

STRUNECKÁ, Anna a Jiří PATOČKA, 2021. *Doba jedová a covidová*. Petrovice: ProfiSales, 318 s. ISBN 978-80-87494-38-7.

The Latest 2023 Cyber Crime Statistics (updated April 2023), 2023. *AAG IT* [online]. London: AAG [cit. 2023-04-16]. Dostupné z: https://aag-it.com/the-latest-cyber-crime-statistics/

TROUSILOVÁ, Alžběta. DNA. *Novinky.cz* [online]. Praha: Borgis; Seznam.cz; ČTK, DPA, Reuters a fotobanka Profimedia [cit. 2022-10-29]. Dostupné z: https://www.novinky.cz/tag/dna-28816

VRÁNOVÁ, Jana. *Zhodnocení dopadu živelních pohrom na stav životního prostředí*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 53 s. (72 584). Dostupné také z: http://hdl.handle.net/10563/24729. Univerzita Tomáše Bati ve Zlíně. Fakulta logistiky a krizového řízení, Ústav krizového řízení. Vedoucí práce Mašek, Ivan.

Výroční zpráva 2021, 2022. *Fakultní nemocnice Brno* [online]. Brno: FN Brno [cit. 2023-04-01]. Dostupné z: https://www.fnbrno.cz/data/files/5697.pdf

WHO Coronavirus (COVID-19) Dashboard, c2023. *World Health Organization* [online]. WHO [cit. 2023-01-07]. Dostupné z: https://covid19.who.int/

Základní pojmy, c2022. *Jaroměř* [online]. Jaroměř: Galileo Corporation [cit. 2022-11-01]. Dostupné z: https://www.jaromer-josefov.cz/prakticke-informace/krizove-rizeni-1/pracoviste-krizoveho-rizeni/zakladni-pojmy/

Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2021, 2022. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Praha: NÚKIB [cit. 2023-04-16]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kybernetick_bezpenosti_2021.pdf

Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020, 2021. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Praha: NÚKIB [cit. 2023-04-16]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ČR	Česká republika
EMA	Evropská léková agentura
EU	Evropská unie
FN	Fakultní nemocnice
HZS	Hasičský záchranný sbor
IZS	Integrovaný záchranný systém
KI	Kritická infrastruktura
MU	Mimořádná událost
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PPK	Pandemický plán kraje
USA	Spojené státy americké
WHO	Světová zdravotnická organizace

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: DOTAZNÍKOVÉ ŠETŘENÍ

1. Jste obeznámen/a s riziky ohrožující kybernetickou bezpečnost?

    a) ANO

    b) NE

2. Probíhá v nemocnici školení zaměstnanců v oblasti kybernetické bezpečnosti?

    a) ANO

    b) NE

3. Jak často toto školení probíhá?

…….

4. Je zabezpečení sítí zdravotnických zařízení podfinancované?

    a) ANO

    b) NE

    c) Nevím

5. Chybí kvalifikovaní lidé v oblasti správy sítí zdravotnických zařízení?

    a) ANO

    b) NE

    c) Nevím

6. Víte, co je to malware a setkal/a jste se s ním?

    a) Vím, ale nesetkal/a

    b) Vím a setkal

    c) Nevím

7. S jakým typem malwaru jste se setkal/a?

…….

8. Setkal/a jste se již někdy s podvodnými emaily?

    a) ANO

    b) NE

9. Stal/a jste se někdy obětí kybernetického útoku?

a) ANO

b) NE

10. Omezila či ohrozila některá kybernetická hrozba Vaši pracovní činnost (náplň práce)?

a) ANO

b) NE

11. Zaznamenal/a jste v období pandemie Covid-19 nárůst kybernetických hrozeb v rámci nemocnice?

a) ANO

b) Spíše ANO

c) NE

d) Spíše NE

e) V nemocnici NE, jinde ANO

12. Myslíte si, že byste mohl/a svým jednáním ohrozit kybernetickou bezpečnost nemocnice z důvodu fyzické i psychické vytíženosti za období pandemie Covid-19?

a) ANO

b) Spíše ANO

c) NE

d) Spíše NE

e) Nevím

13. Je kybernetické prostředí nemocnice zranitelnější při situacích jako je pandemie Covid-19?

a) ANO

b) Spíše ANO

c) NE

d) Spíše NE

14. Bylo by snazší prolomit počítačové zabezpečení nemocnice v období pandemie Covid-19 oproti "běžnému" stavu?

a) ANO

b) Spíše ANO

c) NE

d) Spíše NE

e) Nevím

15. Myslíte si, že je nemocnice dostatečně chráněna proti hackerům a jiným kybernetickým hrozbám?

a) ANO

b) Spíše ANO

c) NE

d) Spíše NE

e) Nevím