# Vliv pandemie na elektronizaci ambulantní zdravotní péče

Šimon Kellner

Bakalářská práce
2022

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

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

Akademický rok: 2021/2022

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

| | |
|---|---|
| Jméno a příjmení: | **Šimon Kellner** |
| Osobní číslo: | **L19140** |
| Studijní program: | **B3909 Procesní inženýrství** |
| Studijní obor: | **Ovládání rizik** |
| Forma studia: | **Prezenční** |
| Téma práce: | **Vliv pandemie na elektronizaci ambulantní zdravotní péče** |

## Zásady pro vypracování

1. Proveďte rešerši dostupných literárních zdrojů v této problematice.
2. Proveďte analýzu současného stavu řešené problematiky.
3. Navrhněte nápravná opatření pro zjištěné nedostatky.

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

Seznam doporučené literatury:


1. BRUCKNER, Tomáš. *Tvorba informačních systémů: principy, metodiky, architektury.* Praha: Grada, 2012. Management v informační společnosti. ISBN 978-80-247-4153-6.
2. BUREŠ, Miroslav et al. *Efektivní testování softwaru: klíčové otázky pro efektivitu testovacího procesu.* Praha: Grada, 2016. Profesionál. ISBN 978-80-247-5594-6.
3. ŠTĚTINA, Jiří. *Zdravotnictví a integrovaný záchranný systém při hromadných neštěstích a katastrofách.* Praha: Grada, 2014. ISBN 978-80-247-4578-7.


Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Pavel Valášek**
Ústav krizového řízení

Datum zadání bakalářské práce: **1. prosince 2021**
Termín odevzdání bakalářské práce: **13. května 2022**

L.S.

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

**Ing. et Ing. Jiří Konečný, Ph.D.**
ředitel ústavu

V Uherském Hradišti dne 1. prosince 2021

# 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: 13. 5. 2022

Jméno a příjmení studenta: Šimon Kellner

.....
podpis studenta

## ABSTRAKT

Tato bakalářská práce se zabývá elektronizací veřejné správy v oblasti zdravotnictví a souvisejících oborů. Nastiňuje současnou situaci v České republice a popisuje aktuálně zavedená softwarová řešení. Přibližuje problematické zavádění nových softwarových nástrojů v průběhu pandemie Covid-19. Dále se zabývá nedokonalostmi daných softwarových nástrojů a navrhuje konkrétní kroky, jak těmto nedostatkům předcházet.



Klíčová slova: elektronizace, státní správa, zdravotní péče, medikament, epidemie, pandemie, Covid-19, informační technologie, informační systém, hacker, malware, kybernetika, dočasná pracovní neschopnost, hygienická stanice, ochrana zdravotnických zařízení, eRecept, eNeschopenka



## ABSTRACT

This bachelor thesis deals with the computerization of public administration in the field of health care and related fields. It outlines the current situation in the Czech Republic and describes the currently implemented software solutions. It presents the problematic introduction of new software tools during the Covid-19 pandemic. It also discusses the imperfections of the software tools and suggests concrete steps to prevent these shortcomings.



Keywords: computerization, state administration, health care, medication, epidemics, pandemics, Covid-19, information technology, information system, hacker, malware, cybernetics, temporary sick leave, hygiene station, protection of medical facilities, electronic prescription, electronic sick leave

V úvodu této práce bych rád poděkoval především panu Ing. Pavlu Valáškovi za výborné vedení bakalářské práce, ochotu pomoci s danou problematikou a za vstřícné jednání.

Také bych rád poděkoval za spolupráci firmě Praktik SW, spol. s r.o., v Olomouci, která se dlouhodobě věnuje oboru informačních technologií se zaměřením na ambulantní sféru zdravotnictví. Firma mi umožnila načerpat důležité informace a nahlédnout do problematiky lékaři využívaných softwarů a státem zaváděných softwarových řešení. Děkuji za cenné a podnětné rady pracovníkům této firmy a také za možnost vykonat zde bakalářskou praxi.

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

# OBSAH

**ÚVOD** ..... **9**
**I TEORETICKÁ ČÁST** ..... **10**
**1 VEŘEJNÉ SLUŽBY A JEJICH ELEKTRONIZACE** ..... **11**
1.1 ELEKTRONIZACE SLUŽEB STÁTNÍ SPRÁVY ..... 11
1.1.1 Elektronizace ..... 11
1.1.2 Elektronizace ve veřejné správě ..... 11
1.1.3 eGovernment ..... 11
1.1.4 Základní registry a Správa základních registrů ..... 12
1.1.7 Portál občana ..... 16
1.2 ELEKTRONIZACE ZDRAVOTNÍ PÉČE ..... 19
1.2.1 Národní zdravotnický informační systém ..... 19
1.2.2 Ambulantní zdravotní péče ..... 19
1.2.3 Distribuce medikamentů ..... 20
1.2.4 Příchod pandemie ..... 20
1.2.7 eRouška ..... 25
**2 ANALYTICKÁ METODA A DŮLEŽITÉ POJMY** ..... **26**
2.1 ANALYTICKÁ METODA WHAT IF ..... 26
2.1.1 Využití metody What if s maticí rizik ..... 26
2.1.2 Matice rizik a související tabulky ..... 26
2.2 POJMY Z OBLASTI ZDRAVOTNICTVÍ ..... 28
2.2.1 Epidemie ..... 28
2.2.2 Pandemie ..... 28
2.2.3 Onemocnění Covid-19 ..... 29
2.3 POJMY Z OBLASTI INFORMAČNÍCH TECHNOLOGIÍ ..... 30
2.3.1 Kybernetika ..... 30
2.3.2 Kybernetická bezpečnost (Cyber Security) ..... 30
2.3.3 Kybernetický prostor ..... 30
2.3.4 Hacker ..... 30
2.3.5 Zákeřný hacker ..... 30
2.3.6 Hacking ..... 31
2.3.7 Vznik hackingu ..... 31
2.3.8 Malware (malicious software) ..... 31
2.3.9 Druhy malwaru ..... 31
2.3.10 Šíření malwaru ..... 31
2.3.11 Spyware ..... 32
2.3.12 Adware ..... 32
2.3.13 Phishing ..... 32
2.3.14 Počítačový virus ..... 32
2.3.15 Trojský kůň ..... 33
2.3.16 Počítačový červ ..... 33
2.3.17 Spam ..... 33
2.3.18 Rootkit ..... 33

2.3.19 Ransomware ..... 33
2.3.20 Medjacking ..... 33
**II PRAKTICKÁ ČÁST ..... 34**
**3 PRAKTICKÁ ČÁST - ÚVOD ..... 35**
3.2 ELEKTRONICKÁ DOČASNÁ PRACOVNÍ NESCHOPNOST ..... 36
3.2.1 Překotný vývoj i nasazení ..... 36
3.2.2 Nespolupráce orgánů státní správy ..... 37
3.2.3 Příchod pandemie ..... 39
3.2.4 Návrh opatření ..... 41
3.3 ERECEPT ..... 42
3.3.5 Návrh opatření ..... 44
3.4 ZABEZPEČENÍ PRACOVIŠTĚ LÉKAŘE (ANALÝZA RIZIK KYBERNETICKÝCH ÚTOKŮ A ÚNIKU INFORMACÍ Z NEMOCNIČNÍCH ZAŘÍZENÍ) ..... 45
3.4.1 Problematika nedostatečné ochrany zdravotnických zařízení ..... 45
3.4.2 Důvody útoků na nemocniční zařízení ..... 46
3.4.3 Hackerské útoky na nemocniční zařízení a související infrastrukturu ..... 46
3.4.4 Analytické zkoumání problematiky ..... 47
3.4.5 Závěr z analyzované problematiky What If ..... 52
3.4.6 Návrhy na opatření ..... 53
3.4.7 Závěr zabezpečení pracoviště ..... 54
3.5 KRAJSKÉ HYGIENICKÉ STANICE ..... 54
3.5.1 Nedostatek pracovníků a zdrojů ..... 54
3.5.2 Útok na hygienické stanice ..... 55
3.5.3 Nařizování karantén a izolací ..... 56
3.5.4 Blokované zprávy KHS ..... 58
3.5.5 Duplicitní zprávy KHS ..... 59
3.5.6 Podvodné SMS s karanténou ..... 61
3.5.1 Návrh opatření ..... 62
**ZÁVĚR ..... 64**
**SEZNAM POUŽITÉ LITERATURY ..... 65**
**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK ..... 73**
**SEZNAM OBRÁZKŮ ..... 74**
**SEZNAM TABULEK ..... 75**

# ÚVOD

Tato práce má za cíl nastínit alespoň část problematiky elektronizace státní správy, a to především v oblasti zdravotnictví. Elektronizace v rámci veřejné správy je dlouhodobě rostoucí trend, který se týká všech odvětví. Díky prudkému rozvoji technologií je neustále potřeba adaptovat i státní správu a její služby. Tento trend se postupně snažilo řešit mnoho vlád napříč politickým spektrem. Vlády se sice snažily dlouhodobě komunikovat s odborníky a řešit problémy elektronizace, nicméně nerazily jednotný postup v rámci tohoto odvětví. Vzhledem k délce reakce na problematiku elektronizace veřejné správy se stávají některé nově zaváděné technologie zastaralými již při zavedení. Státní aparát tudíž zastarává a ne všechny služby fungují naprosto spolehlivě a dle představ státního aparátu či ke spokojenosti občanů, kteří dané služby využívají. Rozdílné vlády sice přicházejí s inovativními změnami v rámci poskytovaných služeb, nicméně mnohá z těchto řešení mají charakter pouze kosmetických úprav. V některých případech vláda zavádí nové neintuitivní platformy, které mají za cíl nahradit dosavadní, což ve výsledku působí chaos mezi uživateli. Na elektronizaci odvětví zdravotnictví měl velký vliv příchod koronavirové pandemie, kvůli které začala vláda překotně zavádět mnoho nových elektronických služeb, jež neprošly žádným nebo jen nicotným zkušebním režimem.

# I. TEORETICKÁ ČÁST

# 1 VEŘEJNÉ SLUŽBY A JEJICH ELEKTRONIZACE

## 1.1 Elektronizace služeb státní správy

### 1.1.1 Elektronizace

Pojem elektronizace se často pojí s pojmem digitalizace, což je proces, při kterém se data převádějí do své elektronické podoby. Pod pojmem elektronizace rozumíme inovaci zaměřenou na komunikační technologie. (IT-Slovník.cz, © 2021)

### 1.1.2 Elektronizace ve veřejné správě

V rámci veřejné správy neustále stoupá zájem o informační technologie a jejich využívání. Veřejná správa stojí o modernizaci a používání nejnovějších technologií pro zrychlení a větší plynulost procesů a agend. Existuje několik projektů, které mají za cíl větší transparentnost a dostupnost veřejné správy. Cílovými skupinami elektronizace veřejné správy jsou kraje, obce, justice, státní zaměstnanci i široká veřejnost. (Ministerstvo vnitra České republiky, © 2021, c)

Realizaci projektů provází nedostatek financí, tento stav zhoršuje podmínky pro jejich uskutečnění. Samotný vrchní ředitel sekce pro informatiku a eGovernment prohlásil v roce 2010 na mikulovské konferenci, že je třeba na tento stav reagovat a přizpůsobit se snížením nákladů na provoz i pořizovacím nákladům. Snižování nákladů se týká i základních projektů v rámci eGovernmentu. (Reichl, © 2021)

V rámci plánovaného zlepšení komunikace ministerstva vnitra má dojít k posílení role České pošty. Česká pošta by měla nově zajišťovat komunikaci mezi složkami Integrovaného záchranného systému a veřejnou správou, která je aktuálně zajišťována službami mobilních operátorů. (Reichl, © 2021)

### 1.1.3 eGovernment

Projekt zvaný eGovernment se pokouší realizovat veřejnou správu za použití nejmodernějších technologií a elektronických nástrojů. Cílem projektu je udělat veřejnou správu levnější, zefektivnit ji a urychlit ji, aby byla pro občany dostupnější. Záměrem je i zjednodušení interakce občana a státní správy. Například se uvažuje o zrušení povinnosti mít u sebe řidičský průkaz při silniční kontrole nebo moci se identifikovat nejen občanským průkazem, ale také třeba mobilním telefonem. (Odbor eGovernmentu, © 2015; Economia, a.s., © 2022)

Mezi lety 2007 až 2013 proběhlo budování základních stavebních kamenů eGovernmentu. Vynik těchto pilířů financovala Evropské unie. Prostředky byly čerpány na základě strategie Smart Administration. (Odbor eGovernmentu, © 2015; Economia, a.s., © 2022)

Mezi prvními vznikla síť Czech POINT, jež se nachází téměř v každé obci. Kterýkoliv občan díky této síti může využívat služby, které dříve fungovaly pouze na konkrétních úřadech, a získávat řadu dokumentů pouze na jednom místě. (Odbor eGovernmentu, © 2015; Economia, a.s., © 2022)

Dalším aspektem projektu eGovernament je systém základních registrů, díky kterému nemusí úředníci žádat o opakované informace od občanů. (Odbor eGovernmentu, © 2015; Economia, a.s., © 2022)

V neposlední řadě je pro eGovernament důležité připojení k internetu, elektronické formuláře a elektronická identita, která je uznávaná v rámci celé Evropy. (Odbor eGovernmentu, © 2015; Economia, a.s., © 2022)

Dalším důležitým pilířem je síť datových schránek, která byla spuštěna, aby sloužila jako nástroj elektronické komunikace a nahradila běžnou písemnou komunikaci pomocí obálek s pruhem. (Odbor eGovernmentu, © 2015; Economia, a.s., © 2022)

### 1.1.4 Základní registry a Správa základních registrů

Dříve byly v rámci každé pobočky úřadu vedeny údaje ve psané formě. Pro každý úřad musel občan vyplňovat formulář s mnohdy duplicitními údaji.

Základní registry změnily referenční údaje na povinné. Pokud jsou údaje vyžadovány agendami, jsou zjišťovány právě v rámci základních registrů. Základní registry fungují již od roku 2012. Jakákoliv změna dat v rámci základních registrů je známa všem příslušným úřadům. (Ministerstvo vnitra České republiky, © 2021, d; Správa základních registrů, © 2022, c)

V základních registrech jsou uvedeny pouze aktuální údaje. Jakýkoliv přístup k informacím zde obsaženým je dokumentován a musí být právně podložen. Na přístup dohlíží Informační systém základních registrů. Osoba, ke které se dané údaje vážou, je o jakémkoli nahlížení do údajů informována. A to buď souhrnně jednou ročně prostřednictvím datové schránky, nebo na vyžádání na Czech POINTu či nově také na Portálu občana. Výpis přístupů k údajům obsahuje data a identifikaci úřadů, které nahlížely, na jaké údaje a za jakým účelem se tak dělo. Bezpečnost základních registrů má

na starost Správa základních registrů. (Ministerstvo vnitra České republiky, © 2021, d; Správa základních registrů, © 2022, c)

Mezi základní registry řadíme:

- Registr osob, ve kterém jsou základní údaje o podnikajících osobách a právnických osobách.
- Dalším registrem je Registr obyvatel, ve kterém jsou obsaženy údaje o fyzických osobách včetně cizinců žijících v České republice.
- Dalším zástupcem základního registru je Registr práv a povinností. Tento registr obsahuje záznamy o jednotlivých přístupech k ostatním registrům a posuzuje, jestli je každý přístup v souladu se zákonem.
- Posledním registrem v základním registru je Registr územní identifikace, adres a nemovitostí, který je zřízený na evidenci státu. Daný registr se zabývá údaji o katastrálních územích, ulicích, pozemcích a postavených objektech.

(Ministerstvo vnitra České republiky, © 2021, d; Správa základních registrů, © 2022, c)

### 1.1.5 Datové schránky

Datové schránky slouží především pro rychlou, levnou a zabezpečenou komunikaci mezi státní správou a občany či právnickými osobami. Podání státní správě prostřednictvím datové schránky jsou zdarma a plně nahrazují doručení psaní s dodejkou. Datové schránky je možné využít také ke komunikaci mezi občany nebo právnickými osobami. Jde sice o placenou službu, avšak ceny jsou výhodnější než u tradičního poštovního styku, o rychlosti nemluvě. (Ministerstvo vnitra České republiky, © 2011; Ministerstvo vnitra České republiky, © 2022, a)

Provoz datových schránek je zdarma, avšak za dlouhodobé archivování zpráv a dokumentů je už potřeba platit. Datové schránky byly zřízeny všem právnickým osobám a tyto je musí ze zákona používat ve styku se státní správou. Občané si mohou zřídit datovou schránku dobrovolně, ale pak ji také musí využívat ve styku se státní správou. Přes zjevné výhody neexistuje mnoho dobrovolných uživatelů. Jelikož ale na datové schránce je eGoverment do značné míry budován, objevují se opakovaně snahy donutit občany zákonem k jejich využívání. Naposledy má například jít o fyzicky podnikající osoby. (Ministerstvo vnitra České republiky, © 2011; Ministerstvo vnitra České republiky, © 2022, a)

#### *1.1.5.1 Informační systém datových schránek a jeho provozní řád*

Informační systém datových schránek je přístupný na informačním webu datových schránek a je řízen za pomoci provozního řádu, který vydává správce informačního systému datových schránek. Tento informační systém se mimo provozního řádu řídí za pomoci zákona č. 300/2008 Sb. a následných vyhlášek č. 193/2009 a 194/2009 Sb. (Ministerstvo vnitra České republiky, © 2011; Ministerstvo vnitra České republiky, © 2022, a)

Systém datových schránek je také dostupný prostřednictvím aplikačního rozhraní pro přímý přístup dalšího softwaru. Tím je například realizován přístup softwaru spisové služby jednotlivých úřadů do systému datových schránek. Aplikační rozhraní využívají také nástroje třetích stran pro práci s datovou schránkou. Například k odesílání Listů o prohlídce zemřelého lékařem na matriční úřad evidující obce. (Ministerstvo vnitra České republiky, © 2011; Ministerstvo vnitra České republiky, © 2022, a)

#### *1.1.5.2 Komunikace mezí Informačním systémem datových schránek a spisovými službami*

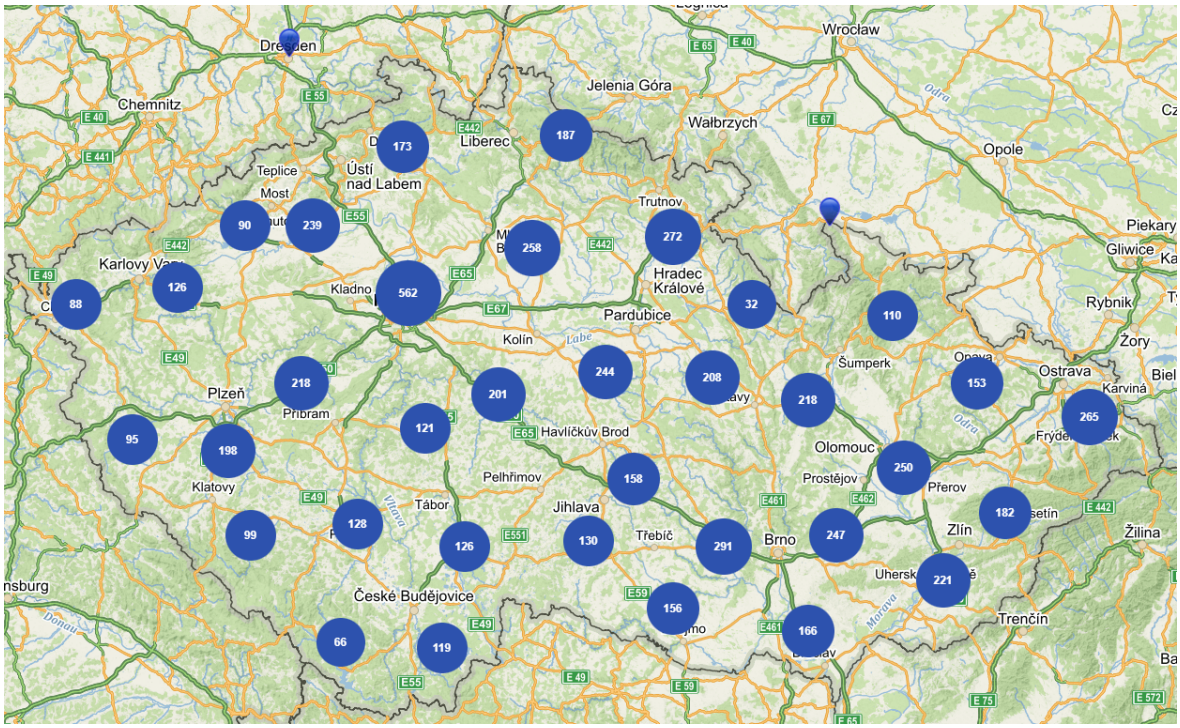
Stát provázal Informačním systémem datových schránek se spisovými službami za pomoci zákona o elektronických úkonech a autorizované konverzi dokumentů č. 300/2008 Sb., který vešel v platnost 19. srpna roku 2008. Účinnosti tento zákon nabyl 1. července roku 2009. (Ministerstvo vnitra České republiky, © 2021, b)

Zásadní změnou tohoto zákona bylo zjednodušení komunikace mezi podnikajícími fyzickými osobami a právnickými osobami a orgány státní moci. Další zásadní změnou je, že veškeré přeposlané dokumenty mezi Informačním systémem datových schránek a spisovými službami jsou považovány za průkazné dokumenty. (Ministerstvo vnitra České republiky, © 2021, b)

Elektronická podatelna, případně elektronické spisové služby nejčastěji zpracovávají přijaté datové zprávy, které pochází od vlastníka dané datové schránky. Tento systém funguje obousměrně, tedy datové zprávy jsou za pomoci elektronických spisových služeb zasílány do Informačního systému datových schránek. (Ministerstvo vnitra České republiky, © 2021, b)

### 1.1.6 Czech POINT

Systém Czech POINT slouží jako kontaktní místo pro přístup občanů k elektronickým službám státní správy. Provozovatelem systému Czech POINT je ministerstvo vnitra. Systém je provozován na kontaktních místech, jako jsou pošty, obecní úřady atp. V České republice je jich provozováno přes šest tisíc a dále je mohou občané využít v zahraničí na zastupitelských úřadech. (Ministerstvo vnitra České republiky, © 2021, a; Ministerstvo vnitra České republiky, © 2022, b)




Obrázek 1 mapa Czech POINT (Ministerstvo vnitra České republiky, © 2022, b)

Kromě přímé návštěvy úřadoven mohou majitelé datových schránek žádat Czech POINT o výpisy z registrů bez nutnosti návštěvy kontaktního místa. (Ministerstvo vnitra České republiky, © 2021, a; Ministerstvo vnitra České republiky, © 2022, b)

Služby, které Czech POINT poskytuje, jsou přibližně tyto:

- poskytování výpisů ze základních registrů a z dalších systémů státní správy (například Katastr nemovitostí);
- podání vůči státní správě, jako například ohlášení živnosti;
- žádosti o změnu údajů v základních registrech;

- správa datové schránky – založení, žádost o vydání přístupových údajů;
- konverze dokumentů z papírové do elektronické podoby a obráceně;
- úřední ověřování podpisů osob či kopií listin.

(Ministerstvo vnitra České republiky, © 2021, a; Ministerstvo vnitra České republiky, © 2022, b)

### 1.1.7 Portál občana

Portál občana funguje jako brána k elektronickým službám nejen státní správy. Do portálu se lze přihlásit za pomoci datové schránky či Identitou občana. Každý občan, který si zřídí přístup k Portálu občana, má možnost komunikovat s úřady elektronicky a spravovat svoje údaje a doklady z jakéhokoliv zařízení připojeného k internetové síti. (Ministerstvo vnitra České republiky, © 2022, c)

Přes portál občana se lze dostat k portálům úřadů, jako jsou Úřad práce, Česká správa sociálního zabezpečení nebo Finanční správa. Dostupné jsou rovněž zdravotní záznamy Očkovacího portálu, eReceptu nebo zdravotních pojišťoven. Postupně přibývají další užitečné aplikace, jako přístupy ke službám samosprávy krajů nebo obcí a dalších. Na tomto portále je také možnost obsluhovat svou datovou schránku. (Ministerstvo vnitra České republiky, © 2022, c)

Vznikem nových projektů v oblasti digitalizace nastala nutnost tyto projekty propojovat a sjednotit je pro jednodušší použití. Portál občana je spojovacím uzlem pro digitalizaci veřejné správy, samosprávy a dalších subjektů. Portál se s postupující digitalizací neustále rozvíjí a poskytuje nové služby. (Ministerstvo vnitra České republiky, © 2022, c)

Služby portálu občana lze využívat též na mobilních zařízeních systému Android a iOS. V současné době je možnost kromě českého jazyka přepnout portál občana také do anglické mutace. (Ministerstvo vnitra České republiky, © 2022, c)

#### *1.1.7.1 Přihlášení*

Za pomoci datové schránky či elektronické Identity občana se lze přihlásit do Portálu občana. Identita občana nabízí pro identifikaci přihlašujícího se občana několik možností:

- elektronický občanský průkaz s čipem vydaný po 1. 7. 2018;
- mobilní klíč k eGovernmentu prostřednictvím načtení QR kódu;

- čipová karta s kvalifikovaným certifikátem První certifikační autority;
- služba CZ.NIC mojeID;
- bankovní identita sedmi tuzemských bank, kterou občané využívají pro přihlášení do internetového bankovnictví;
- International ID Gateway umožňuje přístup k službám české státní správy elektronickou identifikací, vydanou v jiném členském státě EU.

(Ministerstvo vnitra České republiky, © 2022, c; Správa základních registrů, © 2022, a; Internet Info, s.r.o., © 2022; Ústav zdravotnických informací a statistiky ČR, © 2022, c; Magazín Egovernment, © 2022, a; Správa základních registrů, © 2022, b; Česká správa sociálního zabezpečení, © 2021, b)

Přístup k funkcím Portálu občana je však omezen podle úrovně zabezpečení metody, kterou uživatel pro přihlášení zvolí. Přesto, že data jsou dostatečně zabezpečena v jednotlivých informačních systémech veřejné správy, je vhodné eliminovat nebezpečí zneužití dat korektním odhlášením ze služeb Portálu občana. (Ministerstvo vnitra České republiky, © 2022, c; Správa základních registrů, © 2022, a; Internet Info, s.r.o., © 2022; Ústav zdravotnických informací a statistiky ČR, © 2022, c; Magazín Egovernment, © 2022, a; Správa základních registrů, © 2022, b; Česká správa sociálního zabezpečení, © 2021, b)

#### *1.1.7.2 Přihlášení cizinců*

V případě, že cizinec dlouhodobě pobývá v České republice, může se k portálu občana přihlásit za pomoci povolení k pobytu, občanským průkazem, cestovním pasem, vízovým či pobytovým štítkem. Tyto doklady musí být vydány Českou republikou. Občané jiného členského státu EU se mohou přihlásit prostřednictvím International ID Gateway elektronickou identifikací, vydanou v jiném členském státě. (Ministerstvo vnitra České republiky, © 2022, c)

#### *1.1.7.3 Nabízené služby*

Díky Portálu občana se občan efektivně dozví o konci platnosti svých dokladů, ať už prostřednictvím e-mailu, mobilních zpráv či stránky portálu samotné. Občan je tak efektivně informován týdny dopředu, aby si mohl své doklady vyřídit. Funkce Upozornění je standardně nastavena na informování prostřednictvím portálu. Pokud má občan zájem

o jiný druh upozornění, lze jej jednoduše změnit vyplněním patřičných údajů na portále. Po zadání potřebných dat je třeba požadované nastavení aktivovat. (Ministerstvo vnitra České republiky, © 2022, c; Kluska, © 2020)

Portál občana disponuje celou řadou užitečných služeb pro občany, kteří se tento virtuální prostor rozhodnou využívat. Jak již bylo výše zmíněno, lze zde založit novou datovou schránku či ji obsluhovat. Taktéž portál umí archivovat datové zprávy. V rámci elektronizace v průběhu koronavirové pandemie se Portál občana doplnil o nezbytné funkce a informace pro občany, jako jsou přístup k eReceptu a k Očkovacímu portálu. (Ministerstvo vnitra České republiky, © 2022, c; Kluska, © 2020)

Lze zde najít též užitečné informace o vozidlech i řidičích. Zažádání o řidičský průkaz je zde přístupné online, takže občanovi ušetří mnoho času s vyřizováním na úřadu. Nutno podotknout, že služba je určená pro případy, kdy průkazu končí platnost. Výjimkou, kdy tedy není možné o průkaz zažádat online, je jeho zničení, odcizení, změna údajů nebo ztráta. O stavu žádosti je občan informován dle svého výběru ve formuláři přímo na portálu. Každý provozovatel a vlastník vozidla, který se přihlásí do portálu občana, si může zobrazit údaje o vozidle, které vlastní, nebo provozuje. Informace o vozidlech jsou zde nejen aktuální, ale i v rámci záznamů o dříve vlastněných vozidlech, včetně stavu najetých kilometrů. Každý zde přihlášený občan, který je zároveň řidičem, má zde přístup k informacím z registru řidičů i svému aktuálnímu bodovému hodnocení. (Ministerstvo vnitra České republiky, © 2022, c; Kluska, © 2020)

Za zmínku stojí taktéž nejrůznější výpisy, například Výpis z Rejstříku trestů, Výpis z registru obyvatel a Výpis z živnostenského rejstříku. Výpisy získané v rámci portálu jsou v elektronické podobě. Je-li třeba, může si je občan konvertovat do papírové podoby nabízenou službou Czech POINTU. (Ministerstvo vnitra České republiky, © 2022, c; Kluska, © 2020)

Kromě již zmiňovaných informací disponuje portál i informacemi z katastru nemovitostí, přístupem k ePortálu České správy sociálního zabezpečení, přístupem k registračnímu formuláři pro živnostenské oprávnění, přístupem k podání daňového přiznání, přístupem do portálu Úřadu práce, přístupem k Dluhopisům Republiky a přístupem k portálům krajů, měst a obcí. V rámci posledních let taktéž přibyl online test pilota dronu, registrace jeho provozovatele, a dokonce i potvrzení o studiu. (Ministerstvo vnitra České republiky, © 2022, c; Kluska, © 2020)

#### *1.1.7.4 Plánovaný rozvoj*

V současné době přibývají další služby a s rozvojem portálu se počítá i do budoucna. Neustále na portál přibývají další služby, portál občana taktéž komunikuje s obcemi a jejich úřady a jednotlivými ministerstvy. Tato komunikace umožňuje přidávání nových služeb do portálu a jejich modifikaci. (Ministerstvo vnitra České republiky, © 2022, c; Magazín Egovernment, © 2022, b)

Bohužel takovéto jednotné místo sdružující všechny služby nemohou momentálně využívat právnické osoby. Pro ně a pro jejich životní situace se připravuje odlišný Portál podnikatele. Nicméně právnické osoby mohou zatím využívat služby jednotlivých portálů státní správy samostatně. (Ministerstvo vnitra České republiky, © 2022, c; Magazín Egovernment, © 2022, b)

## 1.2 Elektronizace zdravotní péče

Elektronizace českého zdravotnictví pokulhává již delší dobu. Český stát i zdravotnické organizace vynaložili na různé projekty s elektronizací spojené mnoho prostředků s přinejmenším diskutabilními výsledky. Některé projekty nebyly dobře promyšlené, jiné byly ostouzeny mediálně a další neuspěly kvůli nepochopení zdravotnickým personálem. (Řehořek, © 2014)

### 1.2.1 Národní zdravotnický informační systém

Jedná se o státní systém veřejné správy, který zpracovává a shromažďuje osobní a jiné údaje. Dané informace čerpá ze základních registrů, které mají na starost poskytovatelé zdravotnických služeb, ministerstva a orgány veřejné správy. Provozovatelem přístupu k registrům Národního zdravotnického informačního systému je Ústav zdravotnických informací a statistiky České republiky. (Ministerstvo zdravotnictví, © 2021)

### 1.2.2 Ambulantní zdravotní péče

Jedná se o druh zdravotní péče, v rámci níž není nutné pacienta hospitalizovat v nemocničním zařízení. Ambulantní zdravotní péče je poskytována zpravidla v rámci jednoho dne praktickými lékaři primární péče či odbornými specialisty. První zdravotnické ošetření by měli nejprve poskytnout lékaři primární péče, u nichž se pacient registruje. Následně v případě vážnějšího zdravotního problému lékař prvního kontaktu odešle pacienta ke specialistovi. Realita je však často vinou nepřehledné legislativy odlišná.

Pacienti se zdravotním problémem se vyhýbají návštěvě lékaře primární péče a obrací se přímo na specialisty. Protože cena specializované péče je zpravidla dražší než primární péče, vede popsaná svévole pacientů k plýtvání prostředků vyhrazených pro zdravotní péči pacientů České republiky. (Ministerstvo zdravotnictví, © 2021; Medical Tribune, © 2013)

### 1.2.3 Distribuce medikamentů

Distribuci léčiv a prostředků zdravotnické techniky pacientům zajišťuje rozsáhlá síť lékáren. Medikamenty jsou vydávány na lékařský předpis a některé z nich je možné pořídit také ve volném prodeji. Lékařské předpisy mají omezenou platnost. Recept od pohotovostní služby má platnost pouze jeden den od vystavení předpisu. Na určité léky antimikrobiální chemoterapeutika a antibiotika se vztahuje platnost pět dní. Na většinu ostatních předepsaných medikamentů se vztahuje čtrnáctidenní platnost. V případech, kdy je zdravotní stav pacienta stabilizován, a nevyžaduje proto častější návštěvy svého lékaře, vystaví lékař pacientovi opakovací recept, který umožňuje zajistit výdej léku na delší období. Opakovací recept má zpravidla půlroční platnost, ale lékař může platnost zvolit individuálně až na dobu jednoho roku. (Ministerstvo zdravotnictví, © 2021; Státní ústav pro kontrolu léčiv, © 2022, a)

### 1.2.4 Příchod pandemie

Na následujících řádcích se nyní podívejme, jestli a jaký vliv na elektronizaci, především ambulantní sféry zdravotní péče, měl nástup pandemie Covid-19. V jednotlivých oblastech zdravotnictví se totiž rázem objevila řada nových a nečekaných potřeb. Některé, v té době již hotové nástroje, elektronického zdravotnictví získaly zásadně na významu, navzdory předchozímu odmítavému postoji většiny zdravotnického personálu k nim. V oblastech, kde elektronické nástroje chyběly, přispěla pandemická situace k uspíšení přípravy nových řešení.

### 1.2.5 Elektronický recept

#### *1.2.5.1 Zavedení*

Elektronický recept je nástroj Státního ústavu pro kontrolu léčiv, který umožnuje úplnou kontrolu nad všemi medikamenty vydávanými pacientům. Systém plně elektronicky eviduje, který lékař lék předepsal, kdy a kde si jej pacient vyzvedl, zda došlo při výdeji k nějaké náhradě medikovaného preparátu a jaká šarže léčiva byla vydána. V případě

problémů s nějakou konkrétní šarží pak může Státní ústav pro kontrolu léčiv efektivně a cíleně zasáhnout, aby například odvrátil poškození zdraví pacientů. (Veřejná zdravotní pojišťovna, © 2021; Státní ústav pro kontrolu léčiv, © 2018)

Zavedením tohoto nástroje, však byla na lékaře a lékárníky uvalena nepříjemná povinnost plnit systém všemi potřebnými údaji. Nechuť dotčených lékařů a lékárníků způsobila několikaleté odklady nasazení elektronických receptů a zásadní přepracování původního jednoduchého konceptu. Nakonec byla povinnost užívat elektronické recepty definitivně zavedena od roku 2018, ale po dalších protestech se sankce za nepoužívání elektronických receptů odložily až na začátek roku 2019. (Veřejná zdravotní pojišťovna, © 2021; Státní ústav pro kontrolu léčiv, © 2018)

Na začátku roku 2020 již byly obě profesní skupiny s novou povinností smířeny a používání elektronických receptů se stalo běžnou součástí celého zdravotního systému. Když pak na jaře roku 2020 začala sílit pandemie COVID-19, lékaři objevili ohromnou výhodu elektronického receptu. Pacienti se často báli jít k lékaři, ambulantní lékaři nemohli ordinovat kvůli karanténě či izolaci a někteří z nich uvízli v zahraničí a nemohli překročit hranice. Ovšem medikamenty mohli lékaři ordinovat pacientům distančně bez přímého kontaktu s nimi. (Veřejná zdravotní pojišťovna, © 2021; Státní ústav pro kontrolu léčiv, © 2018; Elektronický podpis s.r.o., © 2022)

#### *1.2.5.2 Vystavení receptu lékařem*

Postup lékaře při vystavení elektronického receptu je v podstatě totožný jako při vystavení papírového receptu. Zásadní změnou je absence podpisu na tištěné verzi receptu, ten je nově nahrazen zaručeným elektronickým podpisem. Proto si lékař musí zajistit kvalifikovaný certifikát. Po vyplnění údajů o pacientovi, léku, který je předepisován, a následném doplnění zaručeného elektronického podpisu, odešle recept do centrálního úložiště elektronických receptů. Centrální úložiště vytvoří z přijatých dat elektronický recept a přiřadí mu identifikátor, na základě kterého bude lék pacientovi vydán. V tomto úložišti je elektronický recept dlouhodobě archivován. (Veřejná zdravotní pojišťovna, © 2021; Státní ústav pro kontrolu léčiv, © 2018; Elektronický podpis s.r.o., © 2022)

V případě technických problémů, kdy není možné elektronický recept vypsat, lze vystavit i starší tištěnou formu receptu. Jedná se například o případy, kdy dojde k výpadku elektrické energie, internetového připojení, informačního systému lékaře nebo centrálního úložiště. Poslední případ, kdy lze vystavit původní tištěný recept, je při poskytnutí lékařské první

pomoci. Na takovém náhradním receptu však musí být uveden důvod, proč ho lékař nevystavil v elektronické podobě. Lékárník pak musí recept vložit do centrálního úložiště. (Veřejná zdravotní pojišťovna, © 2021; Státní ústav pro kontrolu léčiv, © 2018; Elektronický podpis s.r.o., © 2022)

#### *1.2.5.3 Vyzvednutí medikamentů*

Pacienti i nadále ve většině případů dostávají papír, který je však pouze průvodkou elektronického receptu. Obsahem je především čárový kód nebo QR kód, který obsahuje identifikátor elektronického receptu lékařem vloženého do centrálního úložiště. Oba kódy slouží lékárníkům k automatizovanému přečtení receptu z centrálního úložiště. Kromě již zmíněné průvodky existují ještě další způsoby, kterými může pacient získat kód elektronického receptu. Státní úřad pro kontrolu léčiv zajistí zaslání identifikátoru pacientovi formou SMS zprávy nebo e-mailem. Zejména služba zaslání SMS je hojně využívaná, ovšem vykazuje mírnou dávku nespolehlivosti, a proto SMS zprávy občas pacientovi nedorazí. To pacient zpravidla zjistí již mimo ordinaci lékaře, ale ten mu může identifikátor nadiktovat po telefonu, často i přímo lékárníkovi. (Veřejná zdravotní pojišťovna, © 2021; Státní ústav pro kontrolu léčiv, © 2018; Elektronický podpis s.r.o., © 2022)

Pokud je pacient v okamžiku vystavení elektronického receptu lékařem dostatečně ztotožněn proti základním registrům, může si léky v lékárně vyzvednout i bez identifikátoru jen na občanský průkaz. Předepsané léky lze vyzvednout díky načtení v elektronické databázi v jakékoliv lékárně. (Veřejná zdravotní pojišťovna, © 2021; Státní ústav pro kontrolu léčiv, © 2018; Elektronický podpis s.r.o., © 2022)

Lékárníci vydávají elektronické recepty na základě údajů z Centrálního úložiště elektronických receptů a doplní zde, že lék již byl vydán, zda došlo k záměně za jiný medikament a jaká je vydávaná šarže léku. Poté již lék nejde vydat v jiné lékárně. Výjimku tvoří opakovací recept pro pacienty, jejichž zdravotní stav je stabilizován. (Veřejná zdravotní pojišťovna, © 2021; Státní ústav pro kontrolu léčiv, © 2018; Elektronický podpis s.r.o., © 2022)

### 1.2.6 Elektronická dočasná pracovní neschopnost

Elektronická dočasná pracovní neschopnost byla již před několika lety zavedena z důvodu zjednodušení a zefektivnění komunikace mezi lékaři, zaměstnavateli a Českou správou sociálního zabezpečení. Bohužel šlo spíše jen o převedení tištěných formulářů do elektronické podoby a ta lékařům ani zaměstnavatelům nepřinášela žádné výrazné zjednodušení. Její užívání lékaři stálo na dobrovolné bázi. (Solitea a.s., © 2021)

Ministerstvo práce a sociálních věcí chtělo pod vedením sociálně orientovaného vedení od července roku 2019 zrušit třídenní karenční dobou dočasné pracovní neschopnosti, a proto muselo přistoupit na politický kompromis. Na nátlak koaličního partnera musela být k 1. lednu 2020 elektronická dočasná pracovní neschopnost užívána povinně a musela být kompletně přepracována tak, aby přinesla jisté zjednodušení lékařům a především zaměstnavatelům. (Solitea a.s., © 2021)

Od zavedení elektronické dočasné pracovní neschopnosti zaměstnanci nemusí podávat žádosti o nemocenské zaměstnavateli a zaměstnavatelé nemusí předávat tyto žádosti České správě sociálního zabezpečení. Všechny tyto úkony řeší nový systém automatizovaně. Zaměstnavatel poskytne České správě sociálního zabezpečení údaje o příjmech zaměstnance pouze tehdy, je-li zaměstnanec neschopen práce déle, než je čtrnáctidenní lhůta. Na základě těchto údajů vyplácí Česká správa sociálního zabezpečení nemocenskou dávku. Lékaři díky elektronické dočasné pracovní neschopnosti mohou přímo zapsat údaje o nemoci pacienta do portálu České správy sociálního zabezpečení. (Solitea a.s., © 2021)

Neustále však zůstává povinnost zaměstnance informovat zaměstnavatele o své pracovní neschopnosti. Pracovní neschopnost zaměstnanec doloží pomocí Průkazu práce neschopného, který musí i nadále vystavovat lékař, ovšem v poněkud jednodušší podobě. Pro správné fungování byl nový systém od října roku 2019 krátce testován v rámci pilotního projektu. Bohužel byla přípravná fáze extrémně krátká a v jejím průběhu se nepodařilo nalézt a odstranit mnoho nedostatků. Na začátku roku 2020 pak proběhl ostrý start nového systému ve značných zmatcích a teprve postupem času se všechny zainteresované strany naučily s ním pracovat. (Solitea a.s., © 2021)

Přes všechny počáteční nesnáze pomohla elektronická dočasná pracovní neschopnost zvládnout nápor vystavování karantén a izolací spojených s pandemií COVID-19. V roce 2021 byl projekt oceněn odbornou porotou v prestižní soutěži IT projekt roku, kterou pořádá Česká asociace manažerů informačních technologií. (Solitea a.s., © 2021)

#### *1.2.6.1 Elektronický portál*

Hlavním komunikačním nástrojem elektronické dočasné pracovní neschopnosti je elektronický portál České správy sociálního zabezpečení. Přes tento portál zaměstnavatelé mohou přímo kontrolovat pracovní neschopnost svých zaměstnanců, aby mohli vykonávat kontrolní činnost dodržování léčebného režimu a vyplácet náhrady mzdy. Zaměstnavatelé si mohou nastavit upozornění na dočasné pracovní neschopnosti svých zaměstnanců do datové či mailové schránky. Informace takto zaměstnavatelem získané jsou z důvodu ochrany osobních údajů značně omezené, například zaměstnavatel se nedozví diagnózu. (Solitea a.s., © 2021)

Pro bezpečné zjištění údajů o zaměstnancích je třeba se do elektronického portálu České správy sociálního zabezpečení autorizovat za pomoci údajů k datové schránce či účtem národní identifikační autority. Jednotlivci se mohou přihlašovat pomocí přihlašovacích prostředků Identity občana. (Solitea a.s., © 2021)

#### *1.2.6.2 Zrušení karenční doby*

Karenční dobou se rozumí kratší lhůta nemoci, při které zaměstnanec žádnou náhradu mzdy nedostává. V českých podmínkách se jednalo o třídenní lhůtu. Náhradu mzdy dostával zaměstnanec až čtvrtý den pracovní neschopnosti. (Hovorková, © 2020)

Karenční doba byla zrušena v červenci roku 2019, a to i přes varování hospodářské komory. Hospodářská komora se obávala především nárůstu nákladů zaměstnavatelů nejen kvůli náhradám mzdy za tyto tři dny, ale taktéž z obavy ze zneužívání a nadužívání nemocenské. (Hovorková, © 2020)

Jak se ukázalo, obavy hospodářské komory byly oprávněné a zrušení karenční doby vedlo ke zvýšení krátkodobé nemocnosti v některých krajích o desítky procent. Naopak při příchodu pandemie COVID-19 pravděpodobně tento krok snížil šíření viru. Vzhledem k tomu, že dočasnou pracovní neschopnost čerpali více zaměstnanci s nižšími pracovními pozicemi, mohlo v případě pokračující třídenní karenční doby dojít k nežádoucímu šíření nemoci z důvodu nedostatku financí na straně zaměstnance. (Hovorková, © 2020)

### 1.2.7 eRouška

Program měla na starost Národní agentura pro komunikační a informační technologie a Ministerstvo zdravotnictví. (Národní agentura pro komunikační a informační technologie, © 2021, b)

Aplikace eRouška měla upozorňovat uživatele, že přišli do kontaktu s osobou nakaženou onemocněním Covid-19. eRrouška patří do projektu Chytrá karanténa, který spadá pod Ministerstvo zdravotnictví České republiky. Program od začátku pandemie využilo 1,7 milionu uživatelů. (Národní agentura pro komunikační a informační technologie, © 2021, b)

Aplikace fungovala na bázi anonymního shromažďování informací o setkávání osob a dodržovala ochranu osobních údajů. Aplikace zaznamenávala blízký kontakt mobilními zařízeními, která taktéž využívala aplikaci eRouška. V případě prokázaného onemocnění Covid-19 uživatel zadal unikátní SMS kód, který obdržel od Krajské hygienické stanice, a ostatní uživatelé, kteří byli v blízkém kontaktu, byli aplikací varováni. Aplikace dle získaných dat za pomocí interního algoritmu sama vyhodnocovala, které kontakty jsou potenciálně rizikové. eRouška byla podporována systémem Android i iOS. Z aplikace se nebylo možné dozvědět, kdo je oním rizikovým kontaktem. (Národní agentura pro komunikační a informační technologie, © 2021, b)

Služba fungovala na bázi standardu pro bezdrátovou komunikaci Bluetooth, který je běžnou součástí chytrých zařízení. Nevyužívala GPS ani nijak jinak nezjišťovala polohu uživatele. Její bezpečnost byla garantována Apple/Google protokolem. Aplikace taktéž úspěšně komunikovala s podobnými evropskými aplikacemi okolních států a z části díky tomu monitorovala i rizikové kontakty ze zahraničí. (Národní agentura pro komunikační a informační technologie, © 2021, b)

K rozhodnutí o pozastavení aplikace eRouška vedla nízká míra využívání. V posledních dnech před pozastavením měla aplikace okolo pěti set tisíc uživatelů a vkládaných informací bylo pouze několik desítek až jednotek denně. Data nasbíraná v rámci aplikace byla smazána k poslednímu dni října roku 2021. Servery a jejich nastavení byly zálohovány a v případě nutnosti může být aplikace opět spuštěna. (Národní agentura pro komunikační a informační technologie, © 2021, a)

# 2 ANALYTICKÁ METODA A DŮLEŽITÉ POJMY

## 2.1 Analytická metoda What if

Jedná se o méně složitou metodu využívanou při ovládání rizik a rozhodování. Tato metoda dostala název po otázce, kterou si analytický tým pokládá. Název analýzy jasně určuje její obsah, a tedy co se může stát, když nastane určitá situace. Tato analytická metoda využívá brainstormingu a diskuse expertů, při kterých se hledají jednotlivá řešení hrozících rizik. V rámci skupinové diskuse se zjišťují nežádoucí účinky konání, hrozících rizik a následně se vytváří opatření pro předejití těmto nežádoucím účinkům. Analytický tým tedy sám navrhuje situace, na které je vhodné reagovat a které představují potencionální riziko. Hlavním účel metody je tedy najít a vytvořit vhodnou reakci na hrozící rizika. (ManagementMania.com, © 2015)

### 2.1.1 Využití metody What if s maticí rizik

Tato metoda se zpracovává do tabulky, která obsahuje několik sloupců, v nichž je na prvním místě příčina. Příčina může být zjišťována brainstormingem, případně mohou příčiny vycházet z metody CLA (Checklist analysis), pokud metodě What if předchází. Dalším bodem v tabulce je následek, jedná se o nastalý stav, který vznikne právě na základě příčiny. Třetím bodem je řešení v podobě preventivního opatření, které má předcházet příčině. Řešení by mělo eliminovat možnosti vzniku příčiny a její opakování. (ManagementMania.com, © 2015)

Doplněním metody What if maticí rizik přibudou v tabulce tři položky, kterými jsou četnost, úroveň rizika, a z těchto dvou sloupců vychází následně celková závažnost. (ManagementMania.com, © 2015)

### 2.1.2 Matice rizik a související tabulky

Matice rizik slouží k vyhodnocení rizik na základě dvou kritérií, povětšinou se jedná o četnost a dopad rizika. (APTIEN.COM, © 2021)

#### *2.1.2.1 Tabulka pro četnost rizika*

V rámci četnosti se používá pravděpodobnostní tabulka, která vytyčí rizika od nepravděpodobných až po vysoce pravděpodobné a patřičně je číselně ohodnotí. Kolonka popisu je následně doplněna dle uvážení analytického týmu. (APTIEN.COM, © 2021)

Tabulka 1 Četnost rizika Ilustrační (APTIEN.COM, © 2021)

| Označení | název | Popis |
|---|---|---|
| I. | Nepravděpodobné | |
| II. | Málo pravděpodobné | |
| III. | Pravděpodobné | |
| IV. | Vysoce pravděpodobné | |

#### *2.1.2.2 Tabulka pro dopad rizika*

Tabulka pro dopad rizika rozděluje rizika od bezvýznamných až po katastrofická a každou úroveň dopadu rizika na zkoumané subjekty označí písmenem vzestupně dle abecedy. Následně každý analytický tým doplní rizika dle oblasti, které se týkají, a závažnosti do tabulky. V tomto případě se metoda zabývá dopadem na společnost, majetek a proces. (APTIEN.COM, © 2021)

Tabulka 2 Úroveň rizika Ilustrační (APTIEN.COM, © 2021)

| Označení | Název | | | |
|---|---|---|---|---|
| | | Společnost | Majetek | Proces |
| A | bezvýznamné | | | |
| B | významné | | | |
| C | kritické | | | |
| D | katastrofické | | | |

#### *2.1.2.3 Tabulka celkové míry rizika*

Tabulka celkové míry rizika pak slouží k vyhodnocení jako klíč dle bodového a abecedního označení daného rizika, podle tabulky četnosti a dopadu rizika. Díky tomu lze zařadit rizika do tří skupin podle závažnosti. Skupiny závažnosti jsou v tabulce barevně vyznačeny, tedy vysokou závažnost označuje červená barva, střední závažnost označuje barva žlutá a zelená barva zvýrazňuje pole s nízkou mírou rizika. Toto seřazení rizik je přehlednější a umožňuje reagovat na rizika adekvátně dle míry jejich závažnosti. (APTIEN.COM, © 2021)

Tabulka 3 Celková míra rizika (APTIEN.COM, © 2021)

| P/D | A | B | C | D |
|---|---|---|---|---|
| I. | 1 | 3 | 6 | 10 |
| II. | 2 | 5 | 9 | 13 |
| III. | 4 | 8 | 12 | 15 |
| IV. | 7 | 11 | 14 | 16 |

## 2.2 Pojmy z oblasti zdravotnictví

### 2.2.1 Epidemie

Epidemie je pojem definovaný podle nemocných lidí ve společnosti. Dle kritérií České republiky pro chřipku se jedná o tisíc šest set až tisíc osm set nakažených lidí v rámci sto tisícové skupiny obyvatel. Za epidemii se nemíní krátkodobý nárůst nemocnosti, ale dlouhodobější stav. V minulosti bylo kritérium pro chřipkovou epidemii vyšší, tedy dva tisíce lidí ve skupině sta tisíc. (Krajská hygienická stanice Moravskoslezského kraje, © 2022, b)

### 2.2.2 Pandemie

Pandemie je pojem definovaný dle hromadného výskytu infekční nemoci na území, které zahrnuje více než jeden stát. Pandemií se tedy míní rozšíření nemoci na velké území, několika států či světadílů zároveň. Oproti epidemii se pandemie nezaměřuje na omezený časový úsek. Pro pandemii je taktéž typické, že bývá způsobena novým typem patogenů,

na které není lidská populace zvyklá, a tudíž proti nim nemá vhodné protilátky. (Roche Czech Republic, © 2017)

### 2.2.3 Onemocnění Covid-19

Onemocnění Covid-19 vyvolává vir s názvem SARS-CoV-2, jedná se o virus patřící mezi koronaviry. Tento virus byl poprvé zaznamenán koncem roku 2019 a jeho šíření označila Světová zdravotnická organizace 11. března 2020 za pandemii. Většina koronavirů se přenáší mezi zvířaty, ale některé z nich mohou infikovat i člověka. (World Health Organization, © 2022; European Centre for Disease Prevention and Control (ECDC), © 2021)

Onemocnění Covid-19 se u většiny infikovaných projevuje mírným, až středně těžkým průběhem bez nutnosti hospitalizace. Někteří infikovaní jsou dokonce úplně bez příznaků. Jiní nakažení ale potřebují krátkodobou, či delší hospitalizaci. Pravděpodobnost komplikací roste s vysokým věkem a jinými zdravotními problémy pacientů. U hospitalizovaných je především potřeba plicní ventilace a ostatních přístrojů na podporu dýchání. Po prodělání onemocnění Covid-19 jsou někteří pacienti méně odolní vůči zápalu plic, či se u nich zvýší možnost infarktů nebo mrtvice, což souvisí se zvýšenou srážlivostí krve. Taktéž se po prodělání onemocnění mohou vyskytnout komplikace související s nervovým systémem. (World Health Organization, © 2022; European Centre for Disease Prevention and Control (ECDC), © 2021)

U malého procenta pacientů se může objevit takzvaný post-covidový syndrom. Tento syndrom se objevuje i u nižších věkových kategorií, a dokonce u lidí, kteří měli lehký průběh onemocnění. (World Health Organization, © 2022; European Centre for Disease Prevention and Control (ECDC), © 2021)

Hlavním rizikem tohoto onemocnění je velmi vysoká rychlost šíření. Covid-19 se šíří převážně kapénkami, které se uvolňují do okolí především při kašlání infikované osoby, ale i u běžného rozhovoru či dýchání. Takto uvolněné kapénky vdechne jiná osoba, a tím se onemocnění dále šíří. Případně se může onemocnění šířit nedostatečnou hygienou, kdy kapénky ulpí na rukou a jsou následně přeneseny dál do těla prostřednictvím očí či úst. (World Health Organization, © 2022; European Centre for Disease Prevention and Control (ECDC), © 2021)

## 2.3 Pojmy z oblasti informačních technologií

### 2.3.1 Kybernetika

Kybernetika vznikla díky rozvoji elektroniky, zejména počítačů, automatiky a telemechaniky. Jedná se o vědu, která se věnuje principům řízení a přenosu informací uvnitř strojů a živých organismů. (Katedra kybernetiky Západočeská univerzita v Plzni, © 2022)

Zakladatelem kybernetiky je Američan a matematik Norbert Wiener, autor knihy: Kybernetika aneb Řízení a sdělování u organismů a strojů. Za součást kybernetiky byla považována například i informatika. (Katedra kybernetiky Západočeská univerzita v Plzni, © 2022)

### 2.3.2 Kybernetická bezpečnost (Cyber Security)

Jedná se o takzvanou informační bezpečnost, která se uplatňuje v jednotlivých počítačích i v sítí. Kybernetická bezpečnost se zabývá ochranou před krádeží informací a majetku a snaží se zamezit nežádoucímu chování počítačů. Kybernetická bezpečnost je systém zajišťující kybernetický prostor, chrání před únikem citlivých a cenných informací. Dále kybernetický prostor zabezpečuje před poškozením či kolapsem, narušením neoprávněné nebo nedůvěryhodné osoby. (CyberSecurity.cz, © 2017)

### 2.3.3 Kybernetický prostor

Pojem kybernetický prostor se definuje jako digitální prostředí, ve kterém je možný vznik, zpracování a výměna informací. Kybernetický prostor též tvoří informační systémy, služby a sítě elektronických komunikací. (Lewik s.r.o., © 2021)

### 2.3.4 Hacker

Jedná se o osobu velice zběhlou v oboru programování. Hacker je většinou odborník v oboru úpravy a manipulace s počítačovými sítěmi a systémy. (AVAST Software s.r.o., © 2022, b)

### 2.3.5 Zákeřný hacker

Jedná se o osobu zneužívající své schopnosti k získávání citlivých informací, neoprávněnému přístupu do sítě a elektronických zařízení. Jeho hlavním cílem je získávání důležitých údajů, kterými jsou například hesla, platební údaje či osobní údaje a fotografie.

Cíli tohoto hackera bývají nejčastěji zisk, zábava či způsobení co největší škody. (AVAST Software s.r.o., © 2022, b)

### 2.3.6 Hacking

Jedná se o cílenou změnu chování softwaru počítače. Hacking se provádí za pomoci programů nebo skriptů. Hacking manipuluje s daty v počítači a získává přístup k informacím v počítači a síti. Malwary, které se používají pro hacking a napadání počítače, jsou: viry, červi, trojský kůň, ransomware a rootkity. Dále se může jednat o hacking za pomoci neautorizovaných změn nastavení v DNS (Domain Name System) serverech. (AVAST Software s.r.o., © 2022, b)

### 2.3.7 Vznik hackingu

V dnešní době je velmi jednoduché provozovat hacking, jelikož hackerské skripty jsou v rámci Internetu volně dostupné ke stažení a modifikování. Při dobré motivaci je poměrně jednoduché naučit se ovládat tyto skripty a využívat je pro získávání cizích osobních údajů, jako jsou například přihlašovací údaje do internetového bankovnictví. Díky dostupnosti hackerských skriptů se zkušenější hackeři učí techniky svých kolegů, které dále rozvíjejí a modifikují stávající skripty. (AVAST Software s.r.o., © 2022, b)

### 2.3.8 Malware (malicious software)

Jedná se o škodlivý software, pokoušející se infikovat elektronické zařízení, jako je mobilní zařízení nebo počítač. Malware je hojně využívaný hackery pro získávání hesel a osobních údajů. Malware může sloužit jako prostředek ke zcizení peněz, případně k nepovolenému přístupu do zařízení. (AVAST Software s.r.o., © 2022, c)

### 2.3.9 Druhy malwaru

Nejčastěji používanými druhy malwaru patří: viry, spyware, adware, phishing, trojští koně, červi, rootkity, ransomware a nepovolené změny v nastavení prohlížeče. (AVAST Software s.r.o., © 2022, c)

### 2.3.10 Šíření malwaru

Nejčastějším druhem šíření malwaru je přes internet a e-mail. Malware se do zařízení dostává pomocí infikovaných webových stránek, prostřednictvím stažených počítačových

her, hudebních souborů, panelů nástrojů, nebo nejrůznějších programů a jakýchkoli jiných stažených dat. (AVAST Software s.r.o., © 2022, c)

### 2.3.11 Spyware

Jedná se o typ malwaru používaný k zjišťování citlivých informací o uživateli napadeného zařízení, převážně se jedná o získání přístupů k bankovním údajům a historii aktivit v zařízení. Je velice obtížné spyware odhalit. (AVAST Software s.r.o., © 2022, i)

Spyware shromažďuje informace o historii prohlížení na internetu a další osobní údaje. Tato citlivá data pak velmi často odesílá bez vědomí napadené osoby na zařízení hackera. Typem spyware je například keylogger, který zaznamenává veškerou aktivitu klávesnice. (AVAST Software s.r.o., © 2022, i)

### 2.3.12 Adware

Jedná se o druh malwaru, který pracuje s obtěžujícími vyskakovacími okny. Tato okna mohou být potencionálně riziková pro dané zařízení. (AVAST Software s.r.o., © 2022, a)

Součástí těchto oken je převážně obtěžující reklama. Tato reklama se zobrazuje většinou ve vyskakovacích oknech, ale může být též obsažena v panelech nástrojů nebo jako součást prohlížeče. (AVAST Software s.r.o., © 2022, a)

Ve většině případů nepředstavuje adware významné riziko, ve výjimečných případech je používán jako spyware. (AVAST Software s.r.o., © 2022, a)

### 2.3.13 Phishing

Phishing je jednou z metod získání citlivých osobních informací. Šíří se za pomoci podvodných emailových zpráv, nebo oběť přesměruje na falešné webové stránky. Phishingové zprávy dokážou věrně napodobit například PayPal, stránky České pošty nebo stránky internetového bankovnictví. Phishing je většinou žádá o aktualizaci, ověření nebo přihlášení do osobního účtu. Zadáním citlivých údajů může dojít ke krádeži identity. (ESET software spol. s r.o., © 2022)

### 2.3.14 Počítačový virus

Jedná se o program (nebo část kódu) s cílem získat kontrolu nad napadeným zařízením a provádět destruktivní akce. K přenosu viru z počítače na počítač může docházet pomocí vnitřních sítí. (AVAST Software s.r.o., © 2022, e)

### 2.3.15 Trojský kůň

Jedná se o druh malwaru, který se tváří jako užitečná část softwaru (hra, hudební skladba). Je však velmi nebezpečný a způsobuje závažné škody a krádeže dat. (AVAST Software s.r.o., © 2022, j)

### 2.3.16 Počítačový červ

Tento typ malwaru je program s množností šíření za pomoci sítě nebo přenosných médií. Tento druh malwaru využívá mnoho částí systému, nebo využívá internetové připojení. Nakažená počítačová zařízení a servery se vyznačují výrazně zpomalenými reakcemi. (AVAST Software s.r.o., © 2022, d)

### 2.3.17 Spam

Jedná se o druh nevyžádané zprávy (převážně reklamy). Pro šíření spamu se tradičně používá emailová komunikace. Spam se může též vyskytovat na blogových stránkách, sociálních sítích a v mobilních zařízeních. Spammeři se s oblibou vydávají za firmy, přátele a rodinné příslušníky. (AVAST Software s.r.o., © 2022, h)

### 2.3.18 Rootkit

Jde se o program pro hackery uzpůsobený tak, aby získal kontrolu nad napadeným zařízením a přístupová práva administrátora. (AVAST Software s.r.o., © 2022, g)

### 2.3.19 Ransomware

Jedná se o malware, který napadá zařízení a zašifruje uživateli důležitá data. Pro šifrování využívá unikátní klíč, který je znám pouze útočníkovi. Hacker za odšifrování dat požaduje výkupné, případně hrozí zveřejněním citlivých údajů v případě neproplacení požadované částky. (AVAST Software s.r.o., © 2022, f; Whalebone, © 2021)

### 2.3.20 Medjacking

Jde se o útoky na zdravotnické přístroje s cílem ohrozit pacienta na zdraví či životě. Hackeři napadají velké či menší zdravotnické přístroje, zařízení vyrábějící komponenty k zdravotnickým zařízením, ba dokonce i kardiostimulátory. Medjacking je hrozbou přicházející v rámci teroristických skupin, ale i hackerů ve službách cizích mocností. (Breene, © 2016)

# II. PRAKTICKÁ ČÁST

# 3 PRAKTICKÁ ČÁST - ÚVOD

Poté, co Českou republiku zasáhla pandemie, se Ministerstvo zdravotnictví České republiky neřídilo v té době platným Pandemickým plánem České republiky. Podle tohoto Pandemického plánu měl být využit informační systém zvaný Informační systém Pandemie. Místo toho za vysokého stupně improvizace živelně vznikaly nové informační systémy pro řízení pandemie COVID-19, nebo se stávající informační systémy upravovaly pro tyto potřeby. (Nejvyšší kontrolní úřad České republiky, © 2022)

V takovém chaosu vznikl například systém elektronických služeb pro řízení epidemie Chytrá karanténa za několik set milionů korun. Amaterismus Ministerstva zdravotnictví byl v mezích možností kompenzován zvýšeným pracovním úsilím příslušníků Armády České republiky, zaměstnanců Ústavu zdravotnických informací a statistiky a Národní agentury pro komunikační a informační technologie. (Nejvyšší kontrolní úřad České republiky, © 2022)

Nyní se pokusme zanalyzovat některé informační systémy pro ambulantní sféru, které vznikaly během pandemie, nebo byly v té době upraveny, aby lépe vyhověly náročným úkolům této těžké zkoušky.

## 3.1 eRouška

Hlavními problémy aplikace eRouška byl nedostatečný apel na občany, aby aplikaci eRouška využívali. Tento prvotní aspekt měl zásadní vliv na oblíbenost a využívání aplikace samotné. Velká část občanů ji neměla zájem ani motivaci používat, někteří občané se taktéž báli, že budou jejich údaje cíleně shromažďovány a následně využívány pro perzekuci. Taktéž došlo k velké demotivaci z důvodu nemalých nároků prvotní verze aplikace na zařízení, což se týkalo převážně rychlého vyčerpání kapacity baterie. (Národní agentura pro komunikační a informační technologie, © 2021, b)

Očekávaná efektivita aplikace spoléhala na její masivní rozšířenost a aktivitu infikovaných uživatelů. O aplikaci byl však u veřejnosti nízký zájem. Přestože počet stažení aplikace dosáhl 1,7 milionu, aktivně využívaných instalací bylo na podzim roku 2021 pouze půl milionu. Přesto, že byly zaznamenány miliony případů nákaz covidem-19, prostřednictvím této aplikace bylo podchyceno jen pět procent případů. S takto získanými daty nebylo dále nijak užitečně nakládáno a to vše přesto, že vývoj a provoz aplikace stál 20 milionů korun.

(Národní agentura pro komunikační a informační technologie, © 2021, b; Národní agentura pro komunikační a informační technologie, © 2021, a)

Aplikace se nedočkala častějšího používání ani s vysokými nárůsty infikovaných. Za úpadek aplikace můžou pravděpodobně i nástroje plošných opatření a v neposlední řadě trasování rizikových kontaktů za značného úsilí pracovníků krajských hygienických stanic. Z těchto důvodů dalo Ministerstvo zdravotnictví podnět k jejímu zastavení do konce října 2021. (Národní agentura pro komunikační a informační technologie, © 2021, a)

## 3.2 Elektronická dočasná pracovní neschopnost

### 3.2.1 Překotný vývoj i nasazení

Od roku 2014 provozovala Česká správa sociálního zabezpečení elektronickou podobu dočasné pracovní neschopnosti. Jak už bylo zmíněno, v roce 2019 se překotně rozhodlo o jejím přepracování a nasazení nového systému už k 1. 1. 2020. Zbudovat zcela nový systém během půl roku je těžko představitelné, jenom testování a pilotní provoz by měly trvat tak dlouho. (Česká správa sociálního zabezpečení, © 2020)

Nové kvapně vypracované řešení nemělo kompatibilní rozhraní s minulým systémem. Dokonce veškeré dočasné pracovní neschopnosti z opouštěného starého systému nebylo možné spravovat prostřednictvím systému nového. Lékařský software tedy musel souběžně komunikovat s oběma systémy elektronické dočasné pracovní neschopnosti podle toho, ve kterém systému byla ta která dočasná pracovní neschopnost založena. (Česká správa sociálního zabezpečení, © 2020)

Místo časově omezeného pilotního provozu byli k novému roku 2020 všichni uživatelé vhozeni do vody nového nedotaženého systému. Chyby, které systém obsahoval nebo které plynuly z nezacvičení pracovníků České správy sociálního zabezpečení či z nepochopení lékařského personálu, se objevovaly a odstraňovaly během jarních měsíců ostrého provozu nového systému. Pracovníci České správy sociálního zabezpečení často vůbec neznali možnosti systému elektronické dočasné pracovní neschopnosti, které poskytoval lékařům, a požadovali po nich úkony, které systém vůbec neumožňoval. Ti pak ve snaze vyhovět, nechápali, proč jim naopak tvůrci jejich informačních systémů odmítají takové požadavky splnit. Docházelo tak ke zbytečně nepřehledné a překotné komunikaci mezi všemi zúčastněnými stranami. (Česká správa sociálního zabezpečení, © 2020)

Ke konfliktům však docházelo i mezi samotnými lékaři. Příčinou bylo politické rozhodnutí povinného užívání nového elektronického systému a obecná nevole lékařů k tomuto nařízení. Z toho důvodu odmítali ambulantní praktičtí lékaři postupovat dle dosavadní zavedené praxe a místo toho se řídili striktně literou zákona. Dříve totiž bylo běžné, že lékař specialista či lékař na pohotovosti pacienta ošetřil a odeslal jej k pokračování léčby k jeho praktickému lékaři s tím, ať pacientovi vystaví dočasnou pracovní neschopnost on. Zákon ale předpokládá, že dočasná pracovní neschopnost je pacientovi vystavena ihned lékařem, který o neschopnosti rozhodl a praktický lékař následně přebírá pacienta do péče s již vystavenou dočasnou pracovní neschopností. Je to i logické. Proč pacient poté, co je po fraktuře na chirurgii ošetřen sádrovým obvazem, musí následně dokulhat ke svému praktickému lékaři pro vystavení dočasné pracovní neschopnosti. Takovou praxi lze jednoznačně označit za nežádoucí. (Medical Tribune, © 2013)

Ze strany ambulantních praktických lékařů šlo nejen o vzdor proti systému, ale také o logickou snahu rozložit nápor s nuceným nasazením nového systému mezi větší počet lékařů. Lékaři specialisté však vinou letité zavedené praxe vůbec neuměli dočasné pracovní neschopnosti zahajovat a v důsledku toho docházelo k dalším zbytečným zmatků a konfliktům. (Ministerstvo zdravotnictví, © 2020)

### 3.2.2 Nespolupráce orgánů státní správy

Na mnoha příkladech z praxe je zřejmé, že při vývoji řady elektronických systémů eGovernmentu spolu různé orgány státní správy příliš nespolupracují. A to přesto, že jejich kompetence se částečně překrývají a konzument od nové služby oprávněně očekává, že ta bude řešit jeho potřeby komplexně bez ohledu na úzce vymezené kompetence jednotlivých úřadů. Podobné chyby jsou patrné také na elektronické dočasné pracovní neschopnosti.

Existuje několik podobných životních situací, které nutí lékaře rozhodnout o tom, že pacient má zůstat určitou dobu doma. Proto mu vystaví nějaký dokument a na jeho základě pacient musí dlít doma a rovněž na jeho podkladě obdrží nějakou náhradu mzdy či sociální dávku. Na všech těchto situacích participuje jako konzument služeb státní správy také zaměstnavatel pacienta. Konkrétně jde o dočasnou pracovní neschopnost, potřebu Ošetřování nemocného člena rodiny, nařízení karantény při podezření na možnou nákazu či nařízení izolace pacienta s vážnou nakažlivou chorobou. Zde se bohužel překrývají kompetence České správy sociálního zabezpečení, podřízené Ministerstvu práce a

sociálních věcí a Krajských hygienických stanic, zřizovaných Ministerstvem zdravotnictví České republiky. (Krajská hygienická stanice Moravskoslezského kraje, © 2022, a)

Důsledkem nespolupráce těchto orgánů byl vznik systému velice úzce zaměřeného jen na dočasnou pracovní neschopnost, a to ještě jen na některé její aspekty. Proto všechny ostatní případy zůstaly postaveny na těžkopádném oběhu papírových formulářů, který je nejen nehodný 21. století, ale také značně nepružný v případě nenadále vynucených změn, jak brzy ukázala příchozí pandemie.

I v takto pojatém řešení však chyběla participace více státních institucí. Náhrady mzdy či sociální dávky pacientům totiž nevyplácí pouze Česká správa sociálního zabezpečení či zaměstnavatel. Svým příslušníkům je přímo bez účasti České správy sociálního zabezpečení vyplácí také Ozbrojené síly České republiky, řízené Ministerstvem obrany České republiky, Vězeňská služba České republiky, spadající pod Ministerstvo spravedlnosti České republiky, Celní správa České republiky, podřízená Ministerstvu financí České republiky, Policie České republiky a Hasičský záchranný sbor České republiky, podřízené Ministerstvu vnitra České republiky a další.

Na takto úzkém výseku elektronizace zdravotní péče, jako je dočasná pracovní neschopnost, se střetl resortismus hned šesti ministerstev a výsledek tomu bohužel odpovídá. Česká správa sociálního zabezpečení si svůj domácí úkol odpracovala, ale k jeho komplexnímu řešení žádný další resort víceméně nepřizvala. Výsledkem je systém, který sice umožní vložit dočasnou pracovní neschopnost příslušníkovi ozbrojených sil či bezpečnostních sborů, ale všechna jeho další funkčnost je okleštěna.

Pacient zpravidla neví zcela přesně, jak zní název a jaké je sídlo jeho zaměstnavatele pro potřeby vystavení dočasné pracovní neschopnosti. Nemalá část pacientů ani přesně neví, jaké zaměstnavatele a případně kolik úvazků u nich má. Proto systém elektronické dočasné pracovní neschopnosti tyto informace lékařům zobrazuje, i když občas neposkytuje úplně relevantní informace, patrně vinou nedodržování ohlašovacích povinností pacientových zaměstnavatelů. Nicméně pro příslušníky ozbrojených sil či bezpečnostních sborů tato služba neposkytuje informaci žádnou. Rovněž při převzetí příslušníka ozbrojených sil či bezpečnostních sborů do péče nemůže lékař elektronický systém použít, musí vše vybavit na základě papírového potvrzení o dočasné pracovní neschopnosti.

### 3.2.3 Příchod pandemie

S příchodem pandemie do České republiky na jaře roku 2022 se plně projevila nekomplexnost a nepřipravenost nasazeného řešení elektronické dočasné pracovní neschopnosti. Vyvstalé problémy se řešily za pochodu, a to v době, kdy systém ani nebyl dostatečně zaběhlý a jeho uživatelé s ním nebyli sžití. Od softwarových firem, které dodávaly programové nástroje lékařům, se očekávala okamžitá implementace ad hoc vymyšlených mnohdy protichůdných změn systému. Rovněž nápor takové zcela nové administrativní zátěže na lékaře byl enormní.

Vyvstala dříve nečekaná potřeba nařizování velkého množství karantén a izolací, což nebylo v takovém rozsahu možné bez nějakého elektronického nástroje, který ovšem chyběl. Využití podobného elektronického nástroje pro dočasnou pracovní neschopnost bylo logickým důsledkem, i když to znamenalo dobudovat chybějící nástroje ke komunikaci mezi Českou správou sociálního zabezpečení, Krajskými hygienickými stanicemi a Ministerstvem zdravotnictví České republiky. Dokonce se uvažovalo o kontrolách dodržování nařízených režimů karantén a izolací příslušníky bezpečnostních sborů. Těm ale rovněž chyběl přístup k informacím tohoto druhu, což bylo jedním z důvodů, proč byly takové kontroly ponechány v kompetenci Krajských hygienických stanic. (Český rozhlas, © 2021)

Jelikož v komunikačním rozhraní elektronické očasné pracovní neschopnosti absentovaly jakékoliv struktury pro podchycení či odlišení karantén nebo izolací a změna v té době čerstvě zavedeného rozhraní nepadala v úvahu, sáhla Česká správa sociálního zabezpečení k jednoduchému opatření. Už v lednu 2020 totiž vydala Světová zdravotnická organizace aktualizaci Mezinárodní klasifikace nemocí pro případy onemocnění COVID-19 a Ústav zdravotnických informací a statistiky České republiky provedl aktualizaci českého vydání tohoto seznamu diagnóz. K tomu byl doplněn kód diagnózy pro pacienta v karanténě. (Ústav zdravotnických informací a statistiky ČR, © 2021; Česká správa sociálního zabezpečení, © 2022)

Tyto nové kódy diagnóz se začaly používat pro odlišení dočasných pracovních neschopností od nařízených karantén a izolací. Onemocnění, pro které nemůže zaměstnanec dočasně vykonávat svou práci, se podle Obecného nařízení o ochraně osobních údajů nemá jeho zaměstnavatel dozvědět, jelikož jde o zvlášť citlivé osobní údaje. Proto výpis dočasných pracovních neschopností pracovníků zaměstnavatele neobsahuje informace o diagnózách. (Škorničková, © 2020)

Aby se zaměstnanci nevyhýbali nařízení karantény nebo izolace z důvodu významného poklesu svých příjmů, byl zaveden mimořádný příspěvek k náhradě příjmů. Očekávaným důsledkem mělo být zvýšení ochoty obyvatel sdělovat rizikové kontakty při trasování, a tím co nejvíce zamezit šíření pandemie. Aby mohli zaměstnavatelé zprostředkovat svým zaměstnancům tento příspěvek od České správy sociálního zabezpečení, museli se nějak o jejich karanténě či izolaci z výpisu dočasných pracovních neschopností dozvědět. Proto měli lékaři tuto informaci kromě vypsání speciální diagnózy vyplňovat také do kolonky určené pro druh povolání. To byla pro ně komplikace jednak zbytečně administrativní a jednak si museli u pacienta poznamenat jeho povolání na jiné místo a zavčas je opravit zpět na skutečné, dříve než by mu vypsali obyčejnou dočasnou pracovní neschopnost. Pokud to opomněli udělat, musí opravu zajistit ručně pracovníci České správy sociálního zabezpečení dříve, než se informace pošle zaměstnavateli. Tyto ruční neautomatizované zásahy vnášely logicky do systému další míru chybovosti. (Česká správa sociálního zabezpečení, © 2021, a)

Jelikož informační systémy lékařů vycházely ze zákona, který neumožňuje souběh několika odlišných dočasných pracovních neschopností u téhož pacienta, musely se tyto nástroje kvůli karanténám a izolacím narychlo přepracovávat. Protože souběh zmíněných případů je naopak zcela běžný. Například pacientovi v dočasné pracovní neschopnosti kvůli fraktuře je později nařízena karanténa kvůli infekční žloutence. Jeho původní dočasná pracovní neschopnost trvá, a to zpravidla i po ukončení režimu karantény. To je zapříčiněno odlišným režimem vyplácení náhrad mezd dle jiného zákonného ustanovení. (Česká správa sociálního zabezpečení, © 2021, a)

Pokud pacient onemocní další chorobou v průběhu dočasné pracovní neschopnosti, zpravidla tato pokračuje s novým kódem diagnózy. Tato zaběhlá praxe však lékařům přinášela konflikty s Českou správou sociálního zabezpečení v situaci, kdy u pacienta s dřívějším podezřením propuklo onemocnění Covid-19. Lékař zpravidla, tak jak se to provánělo u ostatních případů, změnil k nějakému datu diagnózu dosavadní karantény na diagnózu nařízené izolace. Než se patřičně upravil systém na straně České správy sociálního zabezpečení, byl vyžadován postup: nejprve ukončit karanténu, a pak založit novou dočasnou pracovní neschopnost s diagnózou izolace. Doprovodné zmatky a nejednoznačný výklad postupu byly zapříčiněny také nedostatečnou komunikací směrem k lékařům. (Česká správa sociálního zabezpečení, © 2021, a)

### 3.2.4 Návrh opatření

Aby byl jakýkoliv nový informační systém úspěšný, je zapotřebí na něm systematicky pracovat už od okamžiku návrhu. Nestačí jen povzpomínat na všechny formuláře, které se týkají dané problematiky, požadovat jejich převedení do elektronické podoby a jako komunikační platformu mezi klientem a úřadem použít datovou schránku. Je zapotřebí si uvědomit, že nový nástroj má především sloužit, a to zejména občanům. Pouhé stereotypy úředníků nemohou být kvalitním základem pro analýzu požadavků na nové informační řešení. (Bruckner, 2012)

Je důležité navrhnout moderní nástroj do té míry flexibilní, aby byl schopen přizpůsobovat se budoucím změnám, které přináší neustálý vývoj společnosti. Systém musí být navržen jako otevřený pro většinu myslitelných očekávatelných změn jeho parametrů nebo nahrazení některých jeho částí. Proto je nutné k procesu návrhu přizvat všechny „hráče“, kteří budou vstupovat do interakce s chystaným systémem. Nesmí být opomenuta žádná skupina budoucích, třeba jen potencionálních konzumentů jeho služeb. Při návrhu je zapotřebí upozadit pohled zohledňující dosavadní procesy dané instituce a otevřít se novým názorům především budoucích konzumentů připravované služby. Není možné odmítat nové progresivní myšlenky s odkazem na dosavadní požadavky zákona, protože ten bude vždy za realitou jen zaostávat a pravděpodobně bude spíše nutné zamyslet se nad jeho změnou. (Bruckner, 2012)

V každé fázi samotného vývoje a nasazení nového řešení je zapotřebí dostatečně jej testovat. Je hrubou chybou ukvapeně bez dostatečného testování nasazovat nová řešení do provozu, protože podle rozsáhlých výzkumů jsou ceny za opravu závad zjištěných až v ostrém nasazení dvanáctkrát až třináctkrát vyšší než náklady na odstranění chyb nalezených ve fázi vývoje ještě před ostrým nasazením nového projektu do provozu. (Bureš, 2016)

## 3.3 ERecept

### 3.3.1 Portál Externích identit

Přesto, že roku 2017 zřídil Ústav zdravotnických informací a statistiky ČR Národní registr zdravotnických pracovníků, zavedl Státní ústav pro kontrolu léčiv pro potřeby elektronického receptu další rejstříky zdravotnických pracovníků a zdravotnických zařízení pod názvem Portál externích identit. Jejich naplnění probíhalo v roce 2018. Provázely je zmatky, nevole lékařů a nepochopení komplikovaného systému.

Pravděpodobně proto, že ústav nedisponoval emailovými či jinými podobnými kontakty elektronické komunikace na všechny lékaře, rozesílal v průběhu podzimu 2018 fyzickou poštou dopis s jednorázovými prvotními přístupy do nových rejstříků. Bohužel informace byly vytištěné na nekvalitním papíře jehličkovou tiskárnou. Tato kombinace způsobovala velké potíže s čitelností zaslaných údajů. (Ústav zdravotnických informací a statistiky ČR, © 2022, b; Státní ústav pro kontrolu léčiv, © 2022, b; Ústav zdravotnických informací a statistiky ČR, © 2022, a)

### 3.3.2 Přihlašovací údaje

Nyní, když jsou již registry Portálu Externích identit naplněné, je situace klidnější. Složitost, kvůli které zdravotničtí pracovníci systém nechápali a nechápou, však dosud trvá. Ambulantní lékaři mají zpravidla v systému registrovány dvě identity - coby zdravotnický pracovník a také jako zdravotnické zařízení. Každá tato identita disponuje odlišným párem přihlašovacích údajů do webového portálu pro správu těchto identit a dalším párem přihlašovacích údajů do elektronického úložiště elektronických receptů. Do tohoto úložiště vkládá softwarové vybavení lékařů prostřednictvím elektronického rozhraní nové recepty, nebo mění informace o nich. Jedna z těchto identit však má od samého počátku přiděleno ještě GUID. GUID je globální unikátní identifikátor podle specifikace RFC 4122. Tento identifikátor je složen ze třiceti dvou hexadecimálních číslic, tedy číslic 0 až 9 a písmen A až F. Při tvorbě jednoznačného identifikátoru není nutné se spoléhat na žádnou centralizovanou autoritu. K vytvoření jedinečného GUID stačí použít bezplatný online generátor. Asi po roce z nějakého důvodu tatáž identita dostala další nový identifikátor, ale i ten původní zůstal nepochopitelně v platnosti. Pro zabezpečení komunikace protokolem SSL vystavuje Státní ústav pro kontrolu léčiv prostřednictvím vlastí certifikační autority svoje certifikáty odlišné pro každé zdravotnické zařízení. Tento

certifikát uložený v souboru vyžaduje nastavit další heslo. (Ústav zdravotnických informací a statistiky ČR, © 2022, b; Státní ústav pro kontrolu léčiv, © 2022, b; Ústav zdravotnických informací a statistiky ČR, © 2022, a; Gillis, © 2021)

Souhrnně mají tyto dvě identity celkem šest odlišných přihlašovacích jmen a pět hesel, to je celkem jedenáct přihlašovacích údajů. V poslední době bylo do systému dopracováno přihlášení Identitou občana obdobně jako do Portálu občana. Je to sice v souladu s celkovou koncepcí eGovernmentu, ale ambulantním lékařům to situaci nezpřehlednilo. Pouze jim ke stávajícím jedenácti přístupovým údajům přibylo pro identitu zdravotnického pracovníka několik možností s dalšími přístupovými údaji. K identitě zdravotnického zařízení se Identitou občana naopak přihlásit nedá. (Ústav zdravotnických informací a statistiky ČR, © 2022, b; Státní ústav pro kontrolu léčiv, © 2022, b; Ústav zdravotnických informací a statistiky ČR, © 2022, a; Gillis, © 2021)

### 3.3.3 Změny hesel

Autorita zřízená pro generování certifikátů protokolu SSL byla v první verzi velmi špatná. Proces generování certifikátu, který obvykle vrací výsledky okamžitě, trval hodiny až dny. Přestože toto chování bylo neúnosné, odstranění problému si vyžádalo asi rok. Vyřešení přinesla výměna certifikační autority. To ovšem mimo jiné také znamenalo, že dosavadní certifikáty, které měly být platné ještě rok, bylo nutné nahradit novými, a to i přesto, že obě certifikační autority, stará i nová, patřily Státnímu úřadu pro kontrolu léčiv. Protože certifikát měl být ještě platný, uživatel se o problému dozvěděl až z chybového hlášení, kdy systém elektronického receptu starý certifikát začal odmítat.

Na začátku roku 2021 už byli uživatelé celkem uvyklí praxi, že si musí přibližně každý rok a půl generovat nový certifikát SSL s novým heslem. Mnozí z nich už tuto činnost zvládali vlastními silami. Je důležité si uvědomit, že činnost je spojena s identitou zdravotnického zařízení. Během téměř tří let však byli všichni ukolébáni zvyklostí, že ostatní přístupové údaje Portálu externích identit, zejména týkající se zdravotnických pracovníků, se po celou dobu neměnily. Je celkem pochopitelné, že se Státní ústav pro kontrolu léčiv posléze rozhodl z bezpečnostních důvodů začít vyžadovat změnu hesel k identitě Zdravotnického pracovníka. Už méně akceptovatelná byla okolnost, že načasování této změny připadlo na období února až března roku 2021, kdy koronavirová pandemie v České republice procházela jedním ze svých vrcholů.

Důsledkem souhry popsaných skutečností bylo nepochopení a špatný postup naprosté většiny mailem oslovených lékařů. Na výzvu ke změně hesel identity zdravotnického pracovníka se lékaři přihlásili na Portál externích identit, tak jak tomu byli uvyklí kvůli certifikátům SSL, tedy pomocí identity zdravotnického zařízení a této identitě pak změnili heslo. V důsledku docházelo k záměnám poznamenaných hesel mezi zdravotnickým zařízením a zdravotnickým pracovníkem, ale hlavně nedošlo ke včasné výměně hesla, jehož platnost asi do měsíce vypršela definitivně. Oba důsledky, každý zvlášť, vedly k výpadku systém elektronického receptu u zmíněných lékařů.

### 3.3.4 Další využití identit

Identity registrované v Portálu Externích identit jsou postupně využívány dalšími elektronickými zdravotnickými systémy. Nejprve k tomuto kroku přistoupila Česká správa sociálního zabezpečení se svou elektronickou dočasnou pracovní neschopností a později také Informační systém infekční nemoci Ústavu zdravotnických informací a statistiky ČR. (Ústav zdravotnických informací a statistiky ČR, © 2022, b; Státní ústav pro kontrolu léčiv, © 2022, b; Ústav zdravotnických informací a statistiky ČR, © 2022, a)

### 3.3.5 Návrh opatření

Na příkladech této kapitoly je patrno několik problémů. Za všemi je vidět především nedostatečná analýza procesů a v případě duplikování rejstříků i určitá míra resortismu. Vyloženým amaterismem je pak nasazení nekvalitní certifikační autority pro vydávání certifikátů SSL a její nedostatečné testování. Kvalitní testování by odhalilo problém s neúměrnou délkou generování certifikátů zavčas, ještě před nasazením do ostrého provozu. Přechod na novou certifikační autoritu měl, i za cenu obtíží na straně dodavatele softwarového řešení, zachovat funkčnost původních ještě platných certifikátů. (Dostál, © 2020)

Tam, kde nějaký základní rejstřík v rukách státních institucí již existuje, je zapotřebí pouze úprava či jeho rozšíření tak, aby starší rejstřík vyhovoval novým požadavkům místo výstavby dalších nových rejstříků. Při návrhu identit pro přihlašování je potřeba racionálně uvážit, co je cílová skupina v rozumné míře schopna pochopit a nehýřit množstvím identit pro přihlašování. Bezpečnostní pravidla pro tvorbu silných hesel musí být jednotná, aby se uživatel neztrácel v odlišných nastaveních těchto pravidel. Nová řešení, která potřebují certifikáty, musí v maximální míře akceptovat stávající certifikáty uživatele. Jinak se ve velkém množství certifikátů uživatelé brzy začnou ztrácet. (Dostál, © 2020)

## 3.4 Zabezpečení pracoviště lékaře (analýza rizik kybernetických útoků a úniku informací z nemocničních zařízení)

### 3.4.1 Problematika nedostatečné ochrany zdravotnických zařízení

Záměrem této analýzy je poukázat na slabá místa zdravotnických zařízení převážně v oblasti počítačových technologií. Pomoci analýzy What-if bude tento problém blíže specifikován a rozebrán. Tato kapitola neslouží jako negativní kritika aktuálního stavu zdravotnictví, ale jako objektivní zhodnocení daného stavu a možných návrhů pro zlepšení chodu a zkvalitnění ochrany zdravotnických zařízení. Inspirací zabývat se tímto složitým tématem byly předešlé útoky na nemocniční zařízení v České republice, jmenovitě například na Benešovskou nemocnici v roce 2019. Útok na tuto nemocnici ochromil její fungování a způsoboval značné komplikace pro občany, kteří ji v čase napadení potřebovali využít. Pacienti, kteří toto zařízení využívali, byli převezeni do jiných nemocnic a naplánované operace musely být pozastaveny. (VPGC, © 2022)

Nemocnice patří mezi řadu atraktivních cílů hackerských útoků, a to i kvůli chybám samotných zaměstnanců zdravotnických zařízení, které se nevyskytují ojediněle. Vinou těchto chyb a faktu, že se zde vyskytují citlivé a velmi cenné informace o pacientech, se řadí nemocnice mezi velmi atraktivní objekty pro hackery. (CCB spol. s r.o., © 2022)

S nástupem celosvětové pandemie Covid-19 se stalo odvětví zdravotnictví a nově i odvětví pro vývoj vakcín proti tomuto onemocnění terčem častých útoků hackerů. Na dané instituce nově útočí větší skupiny hackerů, které jsou nezřídka z Číny či Ruska. Rostoucí trend hackerských útoků potvrzuje i korporace CheckPoint, která uvedla čtyřiceti pěti procentní nárůst útoků v této oblasti od začátku pandemie. (CCB spol. s r.o., © 2022)

Hackeři používají mnoho různých prostředků pro útok, jedná se o malware typu ransomware, DDoS a botnet útoky či spouštění vzdáleného kódu. Ransomware je v tomto směru mezi hackery velmi oblíbený, protože umožňuje útočníkům zablokovat funkce či informace zdravotnického zařízení a vydírat jej o finanční obnos. (CCB spol. s r.o., © 2022)

Aspektem, který taktéž nahrává potencionálním útočníkům, je stáří počítačů a techniky používaných v nemocnici. Zastaralá technika, neaktualizované prostředí a špatné zabezpečení vede k nízké bezpečnosti počítačových sítí v zdravotnických zařízeních. (CCB spol. s r.o., © 2022)

### 3.4.2 Důvody útoků na nemocniční zařízení

Nemocnice mají velmi složitou infrastrukturu, do které pravidelně investují, to se bohužel nedá říct o oblasti bezpečnosti informačních technologií. Oblast zdravotnictví láká kyberútočníky zvláště kvůli vidině snadno dosažitelného cíle a výdělku, proto zájem o tuto oblast nadále roste. (Whalebone, © 2021)

Důvody útoku mohou být i politické, dle nedávných zjištění se skupina hackerů ze Severní Koreje pokoušela útočit na společnost Johnson & Johnson, která v té době vyvíjela vakcínu proti onemocnění Covid-19. (Whalebone, © 2021)

Předešlé útoky podobného druhu vedly totiž ke kapitulaci vedení nemocnice a přistoupení k požadavkům útočníků, což většinou zahrnuje zaplacení velkého finančního obnosu. (Whalebone, © 2021)

Vedení nemocnice k tomuto chování vede především vědomí, že útočník má v držení extrémně cenné a citlivé údaje. Tyto údaje se týkají informací, které jsou pro pacienty nejen citlivé, ale i životně důležité. Jedná se především o anamnézu a druhy léků, které pacient bere. Nepřistoupení na podmínky hackera by tedy znamenalo nejen riskování úniku citlivých dat pacientů, ale i ohrožení jejich zdraví a v krajních případech i životů. (Whalebone, © 2021)

### 3.4.3 Hackerské útoky na nemocniční zařízení a související infrastrukturu

Roku 2017 zaútočili hackeři za pomoci ransomwaru na Národní zdravotní službu Velké Británie. Tento kybernetický útok postihl okolo dvou set tisíc počítačů, čímž se mu podařilo infikovat šestnáct zdravotnických zařízení. Následkem této infiltrace malwaru došlo k ochromení více než tisíc dvě stě přístrojů důležitých pro fungování tohoto zařízení. (VPGC, © 2022)

Roku 2014 byl veden DDoS útok na dětskou nemocnici v Bostonu. Útok byl veden na stránku dárců. V rámci tohoto útoku přišla nemocnice o šest set tisíc dolarů, zhruba polovina této sumy byla obětována pro znovuobnovení stránky. (VPGC, © 2022)

S rostoucím využíváním technologií v oblasti zdravotnictví roste taktéž riziko medjackingu. Jedná se v podstatě o získání kontroly nad zařízením, které má přímo či nepřímo vliv na život pacienta. Pokusy o tento druh útoku byly například zjištěny ve Spojených státech amerických u anesteziologických strojů firmy General Electric. (VPGC, © 2022)

Roku 2019 postihl ve francouzském městě Montpellier univerzitní zdravotnické středisko phishingový útok. Tento druh útoku vyřadil více než šest set počítačů zdravotnického zařízení. Štěstím bylo, že se jednalo o oddělenou síť počítačů, jinak by hrozil kolaps téměř desetinásobku počítačů. Příčinou byl nebezpečný email, který byl nositelem malwaru. (VPGC, © 2022)

Roku 2018 došlo k úniku citlivých údajů klientů americké zdravotní pojišťovny Independence. Jednalo se o nedbalost jednoho ze zaměstnanců, který citlivé údaje zveřejnil na webu, a tím poškodil skoro sedmnáct tisíc klientů pojišťovny. Tento únik informací byl zjištěn až po téměř dvou měsících. (VPGC, © 2022)

Hackerské útoky se týkají veškeré státní infrastruktury, jak dokazuje například ochromující útok na magistrát města Olomouce v dubnu 2021, tedy v době covidu. (VPGC, © 2022)

S příchodem celosvětové pandemie vzrostly nároky společnosti na rozvoj informačních technologií ve veřejném sektoru a hlavně zdravotnictví. S inovacemi a rozvojem virtuálního prostoru narostl taktéž počet kybernetických útoků. Jak se ukázalo, zvýšená aktivita hackerů a jejich zájem o zdravotnictví dostává zdravotnické pracovníky pod nebývalý tlak. Na zdravotnické pracovníky, kteří jsou už tak zaměstnaní pandemií koronaviru, jsou kladeny nároky i v rámci nových technologií, které se zavádějí v průběhu pandemie. Díky nástupu nových technologií je neustále potřeba lékařské pracovníky poučovat i v rámci bezpečnosti používání těchto služeb, což je v praxi mnohdy opomíjeno. Lze tedy říct, že zdravotnická zařízení jsou velmi lákavými cíli pro potencionální útočníky, kteří nemají morální zábrany útočit na kritickou infrastrukturu a ohrožovat tak zdraví a životy běžných občanů. (Whalebone, © 2021)

### 3.4.4 Analytické zkoumání problematiky

Tabulka 4 Četnosti rizika

| Označení | název | Popis |
|---|---|---|
| I. | Nepravděpodobné | Téměř nikdy |
| II. | Málo pravděpodobné | 1x za 5 let |
| III. | Pravděpodobné | 1x za rok |
| IV. | Vysoce pravděpodobné | 1x měsíčně |

Tabulka 5 Úroveň rizika

| Označení | Název | | | |
|---|---|---|---|---|
| | | Společnost | Majetek | Proces |
| A | bezvýznamné | Spamování počítače při lékařských úkonech | Poškozování počítače těžbou kryptoměn | Zpomalení práce na počítači. |
| B | významné | Dočasné vyřazení počítače | Zničení počítače | Omezení chodu nemocnice v rámci hodin |
| C | kritické | Dočasné vyřazení přístrojů podpory života | Poškození důležitých přístrojů | Omezení chodu nemocnice v rámci týdnů |
| D | katastrofické | Trvalé vyřazení přístrojů podpory života | Trvalé zničení důležitých přístrojů | Trvalé omezení chodu nemocnice |

Tabulka 6 Celková míra rizika (APTIEN.COM, © 2021)

| P/D | A | B | C | D |
|---|---|---|---|---|
| I. | 1 | 3 | 6 | 10 |
| II. | 2 | 5 | 9 | 13 |
| III. | 4 | 8 | 12 | 15 |
| IV. | 7 | 11 | 14 | 16 |

Tabulka 7 Metoda What if s maticí rizik

| P. č. | Příčina | Následek | Opatření | Četnost | Úroveň | Celková závažnost |
|---|---|---|---|---|---|---|
| 1 | Nežádoucí osoba má zájem získat osobní údaje. | Zvýšená možnost napadení. | Kvalitní zabezpečení osobních údajů. | IV. | A | 7 |
| 2 | Nežádoucí osoba má zájem získat část výkonu cizích počítačů. | Vznik rizika těžby. | Firewall, Antimalware, Proškolení zdravotnického personálu. | IV. | A | 7 |
| 3 | Nežádoucí osoba chce otestovat prolomení do sítě. | Napadení počítače. | Firewall, Antimalware, Proškolení zdravotnického personálu. | III. | B | 8 |
| 4 | Nežádoucí osoba má zájem poškodit vnitřní vybavení nemocnice. | Poškození počítače. | Opakované kontroly IT oddělením, proškolení zdravotnického personálu. | II. | C | 9 |
| 5 | Nežádoucí osoba má zájem narušit chod nemocnice. | Zablokování počítačů, zničení přístrojů. | IT oddělení, Antimalware, proškolení lékařů. | III. | C | 12 |
| 6 | Nežádoucí osoba má zájem získat materiál na vydírání. | Zablokování přístupu k důležitým informacím | IT oddělení, Antimalware, proškolení lékařů. | III. | D | 15 |
| 7 | Nežádoucí osoba rozesílá malware. | Narušení chodu počítače. | Antimalware, Firewall, proškolení zdravotnického personálu. | IV. | B | 11 |
| 8 | Firewall je vypnutý. | Možnost průchodu malware do vnitřní sítě | Kontroly IT oddělením a zapnutí Firewall | IV. | A | 7 |
| 9 | Firewall nezablokuje malware. | Možnost průchodu malware do vnitřní sítě | Kontroly IT oddělením a čištění počítače. | IV. | A | 7 |
| 10 | Lékař není poučen. | Možnost stažení malware, úniku informací. | Školení lékařů v oblasti IT bezpečnosti. | IV. | D | 16 |

| P. č. | Příčina | Následek | Opatření | Četnost | Úroveň | Celková závažnost |
|---|---|---|---|---|---|---|
| 11 | Lékař nerozezná malware. | Možnost stažení malware, úniku informací. | Školení lékařů v oblasti IT bezpečnosti. | IV. | D | 16 |
| 12 | Lékař spustí malware. | Malware začne plnit svůj účel. | Školení lékařů v oblasti IT bezpečnosti. | IV. | D | 16 |
| 13 | Lékař neodstraní malware. | Malware bude nadále způsobovat problémy. | Častá kontrola a práce IT oddělení. | III. | D | 15 |
| 14 | Antimalware nezablokuje spuštění malware. | Malware začne plnit svůj účel. | Častá kontrola a práce IT oddělení. | III. | D | 15 |
| 15 | IT technik neodhalí malware a nezablokuje ho. | Malware spustí činnost a způsobí škody. | Výběr kvalitních pracovníků do IT oddělení. | I. | D | 10 |
| 16 | Malware poškodí počítač. | Počítač nelze využít, jsou poškozeny důležité soubory. | Včasné nalezení Malware, proškolení zdravotnického personálu. | III. | B | 8 |
| 17 | Malware použije část výkonu pro těžbu. | Počítač má zpomalené reakce a zasekává se. | Nalezení Malware a jeho eliminace. | IV. | A | 7 |
| 18 | Malware vyřadí počítač dočasně z provozu. | Znemožnění přístupu k důležitým souborům počítače. | Kontroly IT oddělením a čištění počítače. | II. | B | 5 |
| 19 | Nežádoucí osoba získá citlivé údaje. | Problém zneužití důležitých údajů. | Kontroly IT oddělením a dostatečné zabezpečení přístupu. | IV. | B | 11 |
| 20 | Malware se dále šíří v nemocniční síti. | Problém se rozšiřuje na větší okruh zařízení v síti. | Včasné nalezení Malware a jeho eliminace | II. | D | 13 |
| 21 | Malware napadá další počítač. | Malware se replikuje a způsobuje problém v dalším zařízení. | Včasné nalezení Malware a jeho eliminace | II. | D | 13 |

| P. č. | Příčina | Následek | Opatření | Četnost | Úroveň | Celková závažnost |
|---|---|---|---|---|---|---|
| 22 | Malware dočasně vyřadí z provozu elektrickou energii. | Všechny přístroje připojené na elektrickou síť jsou vyřazeny z provozu. | Včasné nalezení Malware a jeho eliminace | II. | D | 13 |
| 23 | Malware dočasně vyřadí z provozu zařízení podpory života. | Pacienti na přístrojích jsou v ohrožení života. | Včasné nalezení Malware a jeho eliminace | I. | D | 10 |
| 24 | Malware se rozšíří z osobního zařízení do nemocniční sítě. | Možnost dalšího šíření v rámci nemocniční sítě. | Zákaz využívání osobních zařízení v rámci zdravotnického zařízení a softwarové omezení USB portů. | III. | A | 4 |
| 25 | Malware zcizí osobní údaje. | Problém zneužití osobních údajů. | Kontroly IT oddělením a dostatečné zabezpečení přístupu. | IV. | B | 11 |
| 26 | Nežádoucí osoba zneužije osobní údaje | Poškození osob | Kontroly IT oddělením a dostatečné zabezpečení přístupu. | II. | B | 5 |
| 27 | Nežádoucí osoba zjistí slabá místa nemocničního areálu | Reálná hrozba napadnutí a teroristického útoku. | Kontroly IT oddělením a dostatečné zabezpečení přístupu. | IV. | D | 16 |
| 28 | Malware vyřadí z provozu energii včetně záložních zdrojů | Ochromení nemocnice. | Mechanické ovládání záložních zdrojů. | I. | D | 10 |
| 29 | Malware naruší průběh operace | Nebezpečí smrti. | Záložní zdroje | II. | D | 13 |
| 30 | Malware vypíše falešný eRecept | Nebezpečí smrti, výroba drog. | Kontrola eRreceptů | I. | D | 10 |

| P. č. | Příčina | Následek | Opatření | Četnost | Úroveň | Celková závažnost |
|---|---|---|---|---|---|---|
| 31 | Přístupové heslo je napsané na obracovce | Nebezpečí vniku nepovolané osoby do zařízení a manipulace s citlivými údaji. | Zákaz znamenání přistupových hesel v okolí počítače, školení zdravotnického personálu. | IV. | B | 11 |
| 32 | Většina pracovníků na oddělení zdravotnického zařízení zná přístupové heslo | Nebezpečí vniku nepovolané osoby do počítače či vnitřní sítě, manipulace s citlivými údaji a možnost nežádoucího přístupu zvenčí. | Zákaz sdělování osobních přístupů dalším osobám, školení zdravotnického personálu. | III. | B | 8 |
| 33 | Pracovník zdravotnického zařízení se neodhlásí a nechá na svém zařízení volný přístup. | Nebezpečí vniku nepovolané osoby do počítače či vnitřní sítě a manipulace s citlivými údaji. | Automatizace odhlašování ze zařízení, proškolení zdravotnického personálu. | IV. | B | 11 |
| 34 | Hacker dostane práci v zdravotnickém zařízení. | Nebezpečí vniku nepovolané osoby do počítače či vnitřní sítě a manipulace s citlivými údaji. | kontrola zaměstnanců | II. | C | 9 |

### 3.4.5 Závěr z analyzované problematiky What If

V rámci této zkoumané problematiky bylo nalezeno sedm příčin s vysokou závažností. Jednalo se o tyto příčiny: Nežádoucí osoba má zájem získat materiál na vydírání, Lékař není poučen v IT, Lékař nerozezná malware, Lékař spustí malware, Lékař neodstraní malware, Antimalware nezablokuje spuštění malware, Nežádoucí osoba zjistí slabá místa nemocničního areálu. Příčin se střední závažností bylo nalezeno jednadvacet. Příčin s nízkou závažností bylo nalezeno sedm.

Proti první příčině, nežádoucí osoba má zájem získat materiál na vydírání, je třeba zvýšit aktivitu IT oddělení, stáhnout kvalitní antimalware, proškolit zdravotnický personál.

Proti druhé příčině, lékař není poučen v IT, je třeba zavést pravidelné povinné školení pro lékaře v oblasti kybernetické bezpečnosti.

Proti třetí příčině, lékař nerozezná malware, je třeba zavést pravidelné povinné školení pro lékaře v oblasti kybernetické bezpečnosti a blokace všech podezřelých emailových příloh.

Proti čtvrté příčině, lékař spustí malware, je třeba zavést pravidelné povinné školení pro lékaře v oblasti kybernetické bezpečnosti a používat kvalitní antimalware.

Proti páté příčině, lékař neodstraní malware, je třeba zvýšit aktivitu IT oddělení, protože lékař či jiný zdravotnický pracovník nemusí vždy efektivně rozlišit, co je malware.

Proti šesté příčině, antimalware nezablokuje spuštění malware, je třeba zvýšit aktivitu IT oddělení, vybrat kvalitnější antimalware a proškolit zdravotnický personál.

Proti sedmé příčině, nežádoucí osoba zjistí slabá místa nemocničního areálu, je třeba zvýšit zabezpečení údajů o areálu a zlepšit činnost IT oddělení.

### 3.4.6 Návrhy na opatření

Velké části problémů lze předcházet častým odborným školením v oblasti kybernetické bezpečnosti, které bude zaměřeno na zdravotnické pracovníky, jelikož právě oni jsou často rozhodujícím faktorem při ohrožení zdravotnického zařízení. Školení pak mohou probíhat i prostřednictvím simulací hackerských útoků, na základě kterých lze učinit kvalitní protiopatření. (VPGC, © 2022; CCB spol. s r.o., © 2022)

Pro kvalitní ochranu zdravotnických zařízení je třeba využívat nejen antimalware, ale i oddělovat jednotlivé části vnitřních sítí, aby nedošlo k narušení celé sítě, ale jen její části. Nutný je též unikátní přístup ke každému přístroji v síti, tedy zabezpečení heslem, které nebude například nalepeno na obrazovce. Dalším důležitým bodem by měla být blokace všech podezřelých emailových příloh. Taktéž je nutné zabezpečit vstup do vnitřní sítě a chránit i jednotlivá důležitá zařízení a přístroje nutné pro bezpečný a plynulý chod nemocnice. Dále je nutné důsledně oddělovat administrativní a kritické systémy. Žádoucí je taktéž aktualizovat software a obměňovat zastaralý hardware. Velmi důležitým bodem je i zálohování všech důležitých dat, tak aby se předešlo možnému riziku zablokování přístupu k těmto údajům a nebyl tak narušen chod nemocnice. (CCB spol. s r.o., © 2022; Breene, © 2016)

### 3.4.7 Závěr zabezpečení pracoviště

Hodnocení úrovně i četnosti rizika je ovlivněno znalostmi analytického týmu, který má zkušenosti s případy z praxe a aktivně řadu z nich řeší a řešil.

Tato kapitola zpracovává možnosti hackerského napadení nemocničního zařízení. Tato rizika práce dále rozvádí a detailně rozebírá za pomoci analýzy What If s maticí rizik. Následným přezkoumáním výstupu z této analýzy vyhodnocuje celková rizika hrozící při současném stavu zdravotnických zařízení. Prioritou pro eliminaci těchto rizik je předcházení příčin jejich vzniku. (VPGC, © 2022; Breene, © 2016)

## 3.5 Krajské hygienické stanice

### 3.5.1 Nedostatek pracovníků a zdrojů

Během koronavirové pandemie násobně narostla práce hygienických stanic především v oblasti trasování rizikových kontaktů a uskutečňování telefonních hovorů při nařizování karantény a izolace. Práce hygienických stanic byla přínosem zejména z důvodu omezení šíření této nakažlivé nemoci. S příchodem epidemie však bylo zjištěno mnoho slabých míst v rámci ochrany veřejného zdraví. Předseda odborné Společnosti hygieny a komunitní medicíny uvedl, že o práci v hygienické stanici mají v průměru zájem jeden až dva lékaři ročně. Jedním ze základních problémů hygienických stanic je nízký zájem o práci v tomto oboru. Jistý vliv na tento fakt má taktéž nízké platové ohodnocení zaměstnanců této sféry. (Němcová, © 2020)

Nedostatek pracovníků v oboru byl nouzově řešen náborem studentů vysokých škol do telefonních center, kde se studenti podíleli na trasování, oznamování nařízené karantény a izolace. Možnosti práce pro hygienické stanice využili převážně studenti lékařských oborů a oborů souvisejících se státní správou. Pro tyto studenty byla práce atraktivnější díky možnosti zpětného uznání odborných praxí, nabytí nových zkušeností a využití znalostí ze svého studia. I přes kladné ohlasy zapojených studentů se většina studentů lékařských fakult chce nadále ucházet o práci převážně v nemocničních zařízeních, a to převážně z důvodu vyššího platového ohodnocení. Finanční ohodnocení nastupujících lékařů v hygienických stanicích a nemocnicích se liší řádově o desítky tisíc korun. Nízký zájem o práci v hygienických stanicích lze pozorovat i na počtu zaměstnanců, který se snížil v rámci posledních deseti let na polovinu. (Němcová, © 2020)

Na jednotlivých krajských stanicích chybí téměř sto čtyřicet zaměstnanců. Ministr zdravotnictví za hnutí ANO Adam Vojtěch sice přislíbil posílení zaměstnanců hygienických stanic, ale i předseda odborné Společnosti hygieny a komunitní medicíny Pavel Dlouhý uvedl, že netuší, z jakých zdrojů počty aprobovaných pracovníků doplnit.

Dalším neřešeným problémem je taktéž vysoký věkový průměr zaměstnaných lékařů, který se pohybuje okolo šedesáti let. (Němcová, © 2020)

Hlavní hygienička Jarmila Rážová věří, že by chybějící zaměstnance mohli doplnit z řad vystudovaných zdravotníků, kteří šli pracovat do jiných odvětví. Sází především na to, že covidová pandemie toto odvětví zpropaguje a zatraktivní. (Němcová, © 2020)

Ministerstvo zdravotnictví České republiky trvale podhodnocuje také materiální podporu pro řízení epidemií a přípravu informačních systémů. Systém, který má umožnit úspěšné řízení epidemií, byl připravován velmi liknavě. Tento Integrovaný systém uživatelů pro Krajské hygienické stanice měl původní termín dokončení v průběhu roku 2019, ale ministerstvo jeho dokončení třikrát posunulo. Proto při vyhlášení pandemie na začátku roku 2020 jednotný komunikační systém v rámci resortu včetně hygienických stanic nebyl k dispozici. (Nejvyšší kontrolní úřad České republiky, © 2022)

Ministerstvo zdravotnictví České republiky od roku 2017 neřešilo značný nedostatek výpočetní techniky Krajských hygienických stanic. Chybělo jim řádově devět stovek kusů výpočetní techniky, kterou na začátku pandemie postrádali pro její zvládání. Tento deficit pokračoval až téměř do konce roku 2020. (Nejvyšší kontrolní úřad České republiky, © 2022)

### 3.5.2 Útok na hygienické stanice

Koncem roku 2021, kdy v České republice probíhala jedna z větších vln pandemie Covid-19, obdržely hygienické stanice na území celého státu desetitisíce dotazů a žádostí. Jednalo se o zbytečné dotazy záměrně odesílané ve velkém množství, kdy iniciátorem bylo seskupení Zlatý špendlík, které založil kontroverzní zpěvák Daniel Landa. Iniciativa přímo vyzývala své členy a podporovatele k zahlcování hygienických stanic stovkami emailů. Sama iniciativa dlouhodobě nazývá práci hygienických stanic během pandemie za zdravotnickou diktaturu. A vyzývala dokonce ke konkrétním dotazům na aktuálně probíhající kontroly. Dle iniciativy měla být odpověď na zbytečný dotaz pro občany přínosnější než kontrolování platných nařízení v souvislosti s onemocněním Covid-19.

Dokonce i sám Daniel Landa na svých účtech v rámci sociálních síti přímo vyzýval k šikaně zaměstnanců hygienických stanic. (Machálková, © 2021)

Problematické je zejména to, že hygienické stanice jsou povinny se obdrženými žádostmi zabývat, a to dle zákona číslo 106/1999 Sb., Zákona o svobodném přístupu k informacím. Kvůli tomuto zahlcení se hygienické stanice musely zabývat odpověďmi na zbytečné dotazy a žádosti, tudíž jim nezbýval dostatek času na trasování, komunikaci s lidmi v souvislosti s vážnými onemocněními, zejména s onemocněním Covid-19, kontroly restauračních zařízení, kontroly bezpečnosti práce a další důležitou činnost. Taktéž vážné a konstruktivní dotazy běžných občanů byly ztraceny v záplavě zbytečných emailů. Kupříkladu pražská hygienická stanice v reakci na toto zahlcení přestala emaily úplně přijímat. (Machálková, © 2021)

Ředitelka jihočeských hygieniků Květoslava Kotrbová uvedla, že jihočeští hygienici obdrželi stovky emailů, u kterých se opakovaly dotazy, kde byli na kontrole v určitém datu, či co určitého data dělali. Z každé emailové adresy obdrželi zhruba deset a více takovýchto emailů. Ředitelka dále uvedla, že je v tomto směru bezradná, protože v rámci zákona o svobodném přístupu k informacím by měli hygienici dotazy zodpovědět, i když jde o evidentní a cílené obstrukce. (Machálková, © 2021)

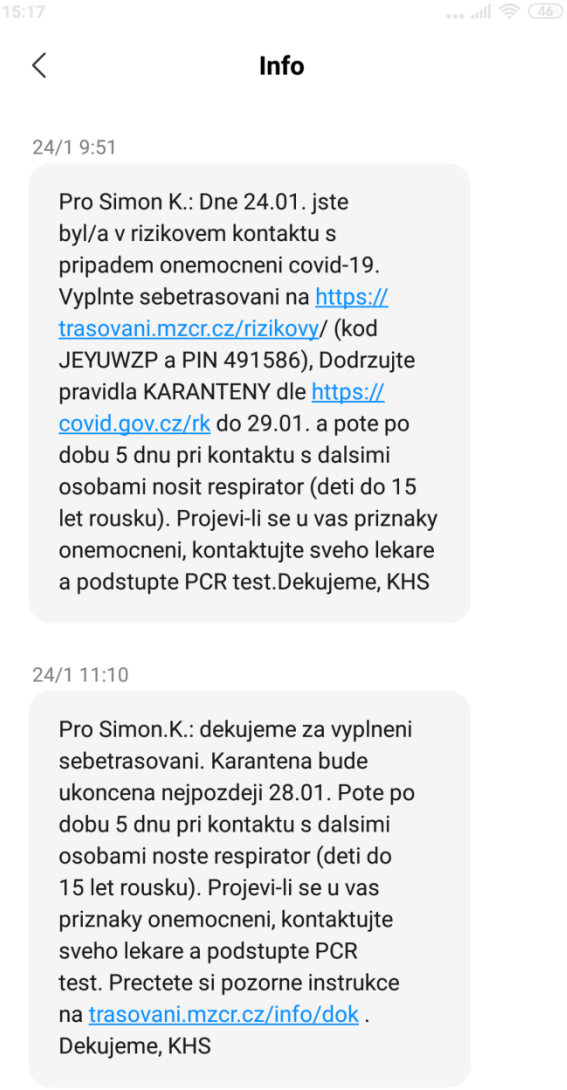
Odborový svaz zdravotnictví a sociální péče České republiky se vůči akci zlatého špendlíku jasně vymezil. Považuje útoky za opovrženíhodné a nebezpečné, zejména kvůli zatěžování pracovníků, kteří mají v souvislosti s pandemií už tak velké množství práce navíc. (Machálková, © 2021)

Ministerstvo zdravotnictví České republiky připsalo tomuto útoku přímý vliv na vyšší hospitalizaci s onemocněním Covid -19. Ministerstvo dokonce podalo na iniciativu Zlatý špendlík trestní oznámení z důvodu podezření ze sabotáže. (Machálková, © 2021)

### 3.5.3 Nařizování karantén a izolací

Pro zefektivnění práce Krajských hygienických stanic byl zaveden samotrasovací formulář a s ním spojený automatizovaný systém, který měl nahradit nedostatek pracovníků Krajských hygienických stanic pro trasování. Bezprostředně po vyplnění rizikových kontaktů v sebetrasovacím formuláři nemocným občanem nebo občanem, který měl s nemocným rizikový kontakt, systém rozeslal textovou zprávu SMS jeho kontaktům s nařízením jejich karantény a výzvou, aby i oni vyplnili sebetrasovací formulář. Po

vyplnění sebetrasovacího formuláře přicházela další SMS zpráva jako potvrzení. (Ministerstvo zdravotnictví, © 2022)




Obrázek 2 karanténa a trasování

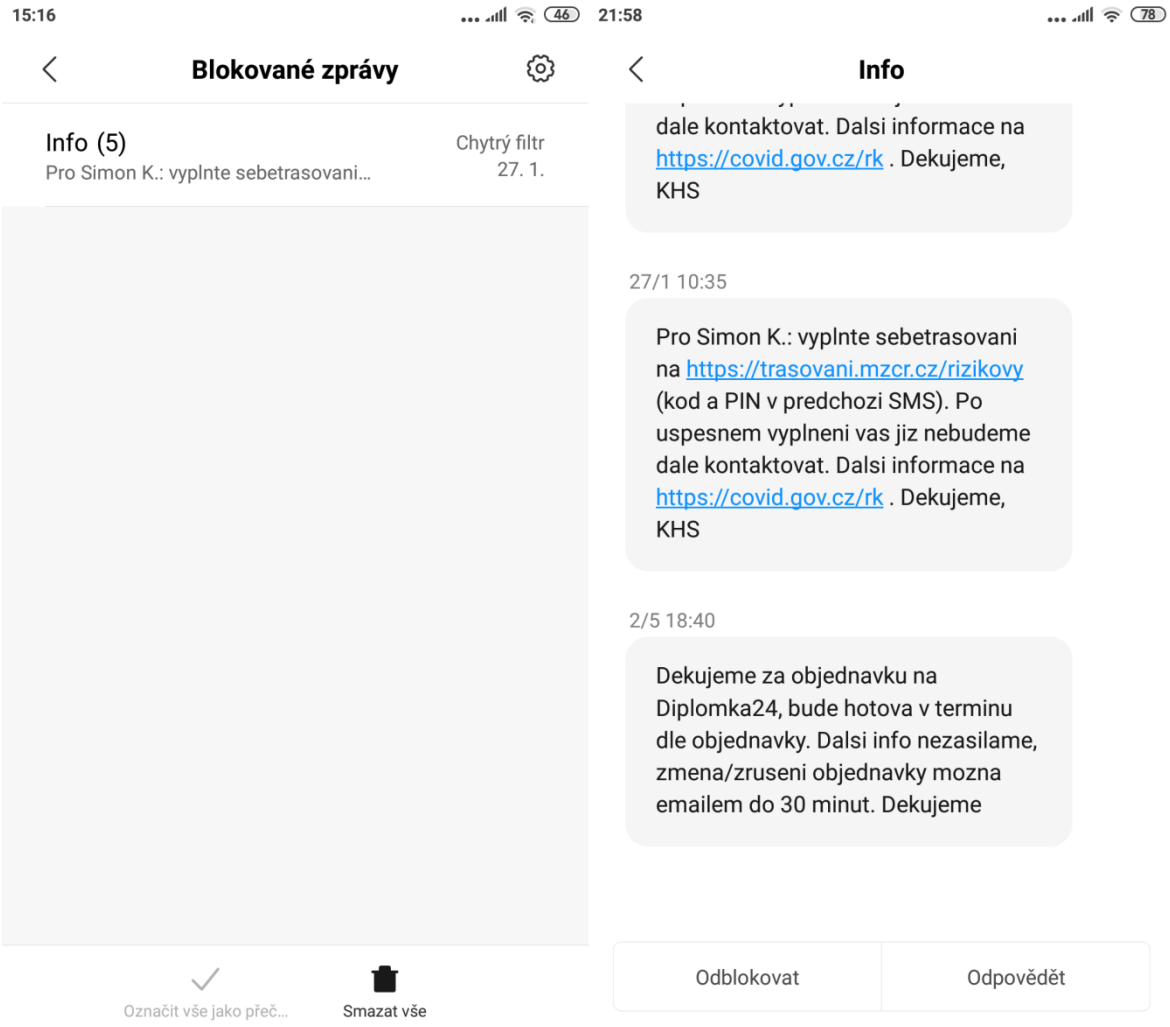
Pokud někdo do samotrasovacího formuláře vyplnil požadavek na vystavení elektronické dočasné pracovní neschopnosti, nebyl o tom nikterak v notifikační zprávě zpraven a ponechán tak v nejistotě. Protože automatizovaný systém nebyl dotažen, museli takové elektronické dočasné pracovní neschopnosti ručně vkládat do systému České správy sociálního zabezpečení pracovníci Krajských hygienických stanic a byli takovou nadbytečnou administrativou neúměrně zavaleni. (Ministerstvo zdravotnictví, © 2022)

Vystavování karanténních elektronických dočasných pracovních neschopností proto vykazovalo několikadenní zpoždění. V průběhu pětidenní karantény tak občanovi nezbylo

než trnout, zda elektronickou dočasnou pracovní neschopnost vystavenu má, či zda dlí doma bez právního důvodu, a tudíž bez náhrady mzdy. Málokdo z nich byl schopen nahlédnout do portálu České správy sociálního zabezpečení, a to buďto přímo, nebo prostřednictvím Portálu občana, a existenci dočasné pracovní neschopnosti zde překontrolovat. I tak by však obdrželi negativní odpověď. Zbytečně proto volali a mailovali na KHS a už tak přetížené pracovníky obtěžovali dotazy, které nemusely vůbec vzniknout, kdyby byl systém automatizován. (Ministerstvo zdravotnictví, © 2022)

### 3.5.4 Blokované zprávy KHS

Oficiální zprávy, které občanům nařizují karanténu či izolaci, jsou bohužel některými zařízeními vyhodnocovány jako škodlivé a nebezpečné. Proto je část zařízení blokuje a je tedy pro některé občany velmi obtížné dozvědět se o nařízeném opatření. V některých případech může kvůli této chybě občan považovat tyto zprávy za falešné, či se dokonce bát přijatý obsah zprávy otevřít a tedy ho i přečíst. K této chybě došlo s vysokou pravděpodobností vinou toho, že telefonní linka 4636 je využívána i pro obchodní nabídky nejrůznějších společností. Při volbě služby pro rozesílání takto závažných textových zpráv nebylo dostatečně uváženo, že dané číslo může být mobilním zařízením vyhodnoceno jako SPAM, či dokonce nebezpečný obsah. Taktéž mohlo dojít k předešlé blokaci přímo uživatelem, kterého takové obchodní nabídky obtěžovaly již v minulosti. (vyhledatcislo.cz, © 2022)



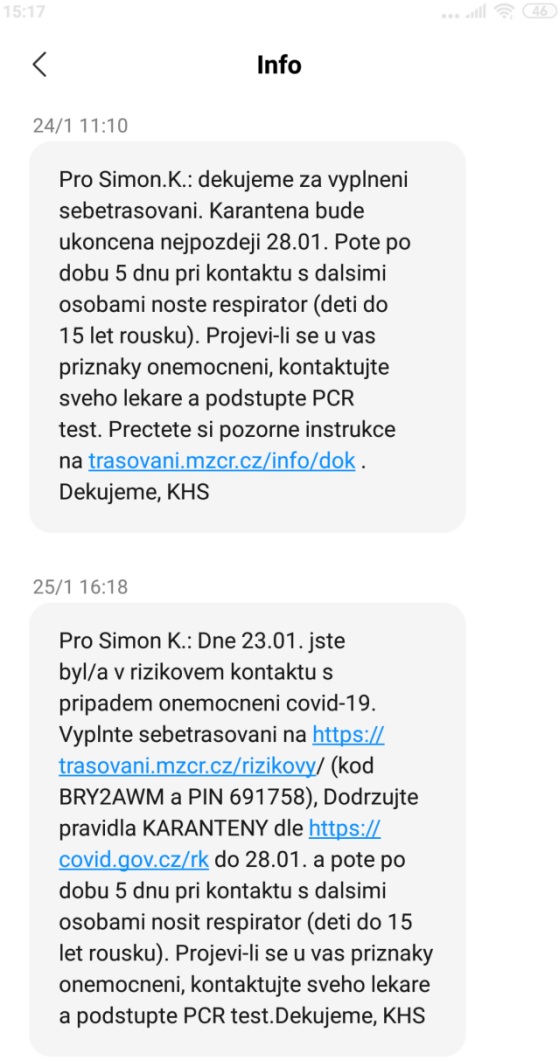

Obrázek 3 blokované zprávy a marketingové nabídky

Dalším problémem je přijetí zprávy občanem, který nedokáže pracovat s informačními technologiemi. Tento problém se týká převážně starších občanů. Takovýto člověk mnohdy není schopen sám vyplnit údaje a informace pro sebetrasování. Někteří dokonce nevlastní mobilní telefon.

### 3.5.5 Duplicitní zprávy KHS

Pokud je občan uvedený jako rizikový kontakt, je kontaktován prostřednictvím SMS, dále je pak vyzván k nahlášení kontaktů osob, se kterými se setkal prostřednictvím sebetrasovacího formuláře. Problém nastane v případě, že je označen jako rizikový kontakt hned několika osobami současně. V takovém případě obdrží hned několik výzev, podle kterých se má sebetrasovat. Navíc pokud vyplní sebetrasovací formulář dříve, než ho někdo jiný stihne uvést ve svém formuláři jako rizikový kontakt, přicházejí mu denně po

celou dobu karantény SMS zprávy, které ho opětovně vyzývají k vyplnění rizikových kontaktů.




Obrázek 4 duplicitní zprávy KHS

Občan je pak v nejistotě, na které zprávy má reagovat a dle kterých přihlašovacích údajů má trasovat své rizikové kontakty. V případě vyplnění trasování podle všech SMS kódů pak vlastně zasílá několikrát duplicitní údaje, čímž problém duplicitních zpráv umocňuje.

Tato závada ukazuje na ledabylou analýzu celé šíře problému a na nedostatečné testování nasazeného řešení.

### 3.5.6 Podvodné SMS s karanténou

Protože SMS zprávy rozesílané hygienickými stanicemi neobsahovaly žádnou přesnější identifikaci odesilatele, pouze strohý podpis „KHS“, a protože nebyla pro rozesílání takových zpráv použita vyhrazená telefonní linka, nabízela se poměrně snadná možnost takové zprávy falešně podvrhnout.

Začátkem roku 2022 dostala část poslanců vládních stran prostřednictvím SMS informaci, že jim byla nařízena povinná karanténa. Zpráva uváděla, že došlo ke kontaktu s osobou pozitivní na Covid-19 a příjemce měl dodržet pětidenní karanténu. Zprávy se na první pohled velmi podobaly textovým zprávám hygienických stanic, obsahovaly dokonce kód k sebetrasování, který měl čtyři znaky a telefonní číslo. V originální SMS od hygieny se jedná o šestimístný kód. (Rambousková, © 2022; ECHO MEDIA, a.s., © 2022)

Vzhledem k tomu, že velká část takto kontaktovaných poslanců vše konzultovala mezi sebou, a dokonce s ministerstvem zdravotnictví, velmi záhy zjistili, že se nejedná o oficiální zprávu nařizující karanténu. Jeden z poslanců, který obdržel tento druh zprávy, byl v té době nemocný doma již týden. Taktéž poslanci zjistili, že unikátní kód, který obdrželi, je totožný s kódy, které obdrželi jejich spolustraníci. Osoba, jež se tímto způsobem pokoušela uvrhnout koaliční poslance do karantény, použila soukromé telefonní číslo. (Rambousková, © 2022; ECHO MEDIA, a.s., © 2022)

Ministerstvo zdravotnictví označilo zprávy za jasné falzifikáty a podalo trestní oznámení. Řada poslanců taktéž zvažuje podání trestního oznámení, jelikož se jednalo o falšování oficiálních zpráv s nařízeními a taktéž zneužívání soukromých kontaktů na poslance a jejich obtěžování. Někteří z poslanců uvedli, že karanténa by měla sloužit k ochraně lidských životů a zdraví občanů, nikoliv jako nástroj pomsty či politického boje. Celá věc je aktuálně vyšetřována policií České republiky. (Rambousková, © 2022; ECHO MEDIA, a.s., © 2022)

Reakcí poslanců vládní koalice v návaznosti na tyto falešné zprávy, které mnohým z nich byly zaslány, je projednávání doplňujících informací v rámci zpráv hygienických stanic. Konkrétně se jedná o kód, který by každá zpráva měla obsahovat a který by následně bylo možné ověřit přímo na stránkách hygienické stanice. Pro ověření platnosti přijaté SMS lze nahlédnout na internetové stránky ministerstva zdravotnictví. (Rambousková, © 2022; ECHO MEDIA, a.s., © 2022)

### 3.5.1 Návrh opatření

Zásadní pomoc tomuto dříve opomíjenému sektoru našeho zdravotnictví by přineslo rozsáhlé investování do infrastruktury hygienických stanic, ať už se jedná o dostatečnou technickou vybavenost či adekvátní platové ohodnocení kvalifikovaných zaměstnanců. Platový nárůst je neopominutelným předpokladem pro zatraktivnění profese pro profesionály z řad lékařů, kterých se hygienám nedostává. (Němcová, © 2020)

Útok na tuto infrastrukturu šlo jen těžko předpokládat. Iniciativa Zlatý špendlík ukázala, jakým způsobem lze tato zařízení jednoduše a efektivně napadnout a omezit jejich fungování. Proti velkému množství požadavků se lze částečně bránit zapracováním algoritmů strojového učení do programu spisové služby, které by rozpoznaly obtěžující dotazy a adekvátně by na ně reagovaly. Tyto algoritmy by mohly rozpoznat dříve zodpovězené typy otázek a starší odpovědi použít, nebo by mohly odpovědi na některé jednodušší otázky umět samy vyhledat a zodpovědět. Takové služby expertního rázu by mohli výrobci spisových služeb vyvinout a nabízet i jiným státním institucím, které podobnou zkušenost již mají nebo by mohli rovněž být podobným způsobem atakovány.

Taktéž by měla existovat legislativní opora pro například prodloužení lhůt pro odpovědi na přijímané dotazy v období extrémního vytížení pracovníků v době nouzového stavu či pandemické pohotovosti. Protože obtěžování nadměrným množstvím dotazů není jen výsadou Krajských hygienických stanic, měla by být konkrétně legislativně ošetřena právní odpovědnost osob nebo skupin osob, které svými dotazy instituce přetěžují.

Zvláštní pozornost je zapotřebí věnovat kvalitě služeb pro notifikaci prostřednictvím SMS zpráv. Doplnění zprávy unikátním odkazem pro ověření autenticity může být jedním z prvků řešení. Dalším krokem by bylo odesílání zpráv z k tomu výhradně zřízené telefonní linky, která nebude využívána jiným, například komerčním způsobem. Není možné nacházet nařízení karantény se silnými právními důsledky mezi reklamou na elektroniku atp. Ideální by bylo, aby každá státní instituce měla k tomu účelu zřízenou linku vlastní. Jinak může být občan zmaten, že mu z linky, která jej pravidelně vyzývá k platbě daně z nemovitostí, přichází urgentní varování Hasičského záchranného systému, totiž že v důsledku hrozící povodně je nutná evakuace.

Formulář pro sebetrasování byl jistě ulehčením zátěže Krajských hygienických stanic díky automatizovanému vyzývání dalších rizikových kontaktů, ale byl také ukázkou nedostatečné analýzy celého procesu. Pro úspěšné zvládnutí pandemie měl automatizovaný

systém rizikovým kontaktům, které požádaly o vystavení karanténní dočasné pracovní neschopnosti, tyto vystavovat a posléze ukončovat automatizovaně. Pouze v případech, kdy by měl automatizovaný systém problémy třeba s adresou pacienta nebo jeho zaměstnavatelem, by pak vyvstala práce pro pracovníka Krajské hygienické stanice.

# ZÁVĚR

Tato práce nastínila základní myšlenky problematiky elektronizace v období probíhající celosvětové pandemie Covid-19. Především se zaměřovala na zdravotnictví a s ním spojené obory, dále pak na informační technologie. Práce dále popsala některé kroky politické reprezentace související s oblastí zdravotnictví a elektronizací. Taktéž se práce zabývala elektronickými nástroji, které jsou součástí státní správy a jsou v rámci zdravotnictví využívány. V rámci praktické části je popsána problematika jednotlivých sektorů a návrhy řešení daných problematik. Taktéž jsou zde vypsány problémy konkrétních služeb a odvětví souvisejících se zdravotnictvím.

Zdravotnictví je oblastí nejvyšší priority a dlouhodobě se do něj investuje mnoho finančních prostředků, bohužel se však peníze většinou nepoužívají na obměnu starších počítačů či zabezpečení lékařských strojů a zařízení. Fakt, že v rámci informačních technologií mají nemocniční zařízení značné rezervy, je bohužel hojně využíván taktéž nejrůznějšími útočníky a je třeba ho aktivně řešit. Nedostatečnou připravenost nemocničních zařízení na nejrůznější útoky, ale i běžnou práci se softwarem umocnil taktéž příchod pandemie a polovičatá rozhodnutí v rámci nasazování nových softwarových nástrojů pro zdravotníky.

Též je smutným faktem, že i přes upozornění Nejvyššího kontrolního úřadu stále neexistuje zapracování nové informační podpory do Pandemického plánu České republiky. Ministerstvo zdravotnictví nezapracovalo informační podporu ani v rámci informační koncepce Ministerstva zdravotnictví. Přestože v tomto směru bylo do zdravotnictví investováno mnoho finančních prostředků, hrozí, že program Chytré karantény nebude v rámci dalších epidemií využit. (Nejvyšší kontrolní úřad České republiky, © 2022; Štětina, 2014)

Příchod pandemie do tohoto odvětví dostal větší množství finančních prostředků a dal vzniknout mnoha softwarovým řešením, bylo by tedy smutné, kdyby byla daná řešení po skončení pandemie zrušena a zapomenuta. (Nejvyšší kontrolní úřad České republiky, © 2022)

# SEZNAM POUŽITÉ LITERATURY

APTIEN.COM. © 2021. Risk matrix: activation and settings. aptien.com. [Online] 2021. [Citace: 30. 4 2022.] https://aptien.com/en/kb/articles/risk-matrix-activation-and-settings.

AVAST Software s.r.o. © 2022, a. Adware. avast.com. [Online] 2022, a. [Citace: 30. 4 2022.] https://www.avast.com/cs-cz/c-adware.

AVAST Software s.r.o. © 2022, b. Hacker. avast.com. [Online] 2022, b. [Citace: 29. 4 2022.] https://www.avast.com/cs-cz/c-hacker.

AVAST Software s.r.o. © 2022, c. Malware. avast.com. [Online] 2022, c. [Citace: 29. 4 2022.] https://www.avast.com/cs-cz/c-malware.

AVAST Software s.r.o. © 2022, d. Počítačový červ. avast.com. [Online] 2022, d. [Citace: 30. 4 2022.] https://www.avast.com/cs-cz/c-computer-worm.

AVAST Software s.r.o. © 2022, e. Počítačový virus. avast.com. [Online] 2022, e. [Citace: 30. 4 2022.] https://www.avast.com/cs-cz/c-computer-virus.

AVAST Software s.r.o. © 2022, f. Ransomware. avast.com. [Online] 2022, f. [Citace: 30. 4 2022.] https://www.avast.com/cs-cz/c-ransomware.

AVAST Software s.r.o. © 2022, g. Rootkit. avast.com. [Online] 2022, g. [Citace: 30. 4 2022.] https://www.avast.com/cs-cz/c-rootkit.

AVAST Software s.r.o. © 2022, h. Spam. avast.com. [Online] 2022, h. [Citace: 30. 4 2022.] https://www.avast.com/cs-cz/c-spam.

AVAST Software s.r.o. © 2022, i. Spyware. avast.com. [Online] 2022, i. [Citace: 30. 4 2022.] https://www.avast.com/cs-cz/c-spyware.

AVAST Software s.r.o. © 2022, j. Trojský kůň. avast.com. [Online] 2022, j. [Citace: 30. 4 2022.] https://www.avast.com/cs-cz/c-trojan.

Breene, Keith. © 2016. What is medjacking? weforum.org. [Online] 2016. [Citace: 30. 4 2022.] https://www.weforum.org/agenda/2016/10/medjacking-health-cyber-risk-explainer/.

Bruckner, Tomáš. 2012. Tvorba informačních systémů: principy, metodiky, architektury. Praha : Grada, 2012. 978-80-247-4153-6.

Bureš, Miroslav. 2016. Efektivní testování softwaru: klíčové otázky pro efektivitu testovacího procesu. Praha : Grada, 2016. 978-80-247-5594-6.

CCB spol. s r.o. © 2022. Útoky na zdravotnická zařízení ještě zdaleka nejsou na vrcholu. systemonline.cz. [Online] 2022. [Citace: 25. 4 2022.] https://www.systemonline.cz/it-security/utoky-na-zdravotnicka-zarizeni-jeste-zdaleka-nekonci.htm.

CyberSecurity.cz. © 2017. Kybernetická bezpečnost (Cyber Security). CyberSecurity.cz. [Online] 2017. [Citace: 29. 4 2022.] https://cybersecurity.cz/basic.html.

Česká správa sociálního zabezpečení. © 2020. Nejčastěji kladené dotazy pro vývojáře lékařských SW. cssz.cz. [Online] 9. 4 2020. [Citace: 30. 4 2022.] https://www.cssz.cz/documents/20143/178393/Nejcasteji_kladene_dotazy_pro_vyvojare_lekarskych_SW_20200409.pdf/6221c459-34f6-ddd7-9298-4e142632ff75.

Česká správa sociálního zabezpečení. © 2021, a. Mimořádný příspěvek při nařízené karanténě (tzv. izolačka) - postupy lékařů a zaměstnavatelů. cssz.cz. [Online] 18. 3 2021, a. [Citace: 15. 4 2022.] https://www.cssz.cz/-/mimoradny-prispevek-pri-narizene-karantene-tzv-izolacka-postupy-lekaru-a-zamestnavatelu.

Česká správa sociálního zabezpečení. © 2021, b. Revoluce v komunikaci se státem na obzoru - vyzkoušeli jste si již v praxi svou elektronickou identitu? cssz.cz. [Online] 22. 2 2021, b. [Citace: 30. 4 2022.] https://www.cssz.cz/web/cz/-/revoluce-v-komunikaci-se-statem-na-obzoru-vyzkouseli-jste-si-jiz-v-praxi-svou-elektronickou-identitu-?inheritRedirect=true&redirect=https%3A%2F%2Fwww.cssz.cz%2Fweb%2Fcz%2Fvyhledavani%3Fp_p_id%3Dcom_liferay_portal_search_web_po.

Česká správa sociálního zabezpečení. © 2022. Nemocenská statistika. cssz.cz. [Online] 2022. [Citace: 30. 4 2022.] https://www.cssz.cz/nemocenska-statistika#section_5.

Český rozhlas. © 2021. Kontroly karantén? ‚Není garance, k čemu bude policie data od hygieny používat,' říká právní expert. irozhlas.cz. [Online] 2021. [Citace: 30. 4 2022.] https://www.irozhlas.cz/zpravy-domov/policie-kontrola-karanteny-covid-19-ochrana-osobnich-udaju-jan-voboril_2103241218_kro.

Dostál, Dalibor. © 2020. Zpackaná digitalizace. Zdravotnictví předvedlo, jak nemá vypadat. businessinfo.cz. [Online] 10. 6 2020. [Citace: 30. 4 2022.] https://www.businessinfo.cz/clanky/zpackana-digitalizace-zdravotnictvi-predvedlo-jak-nema-vypadat/.

Economia, a.s. © 2022. Řidičák už brzy nebude potřeba, občanka postačí elektronická, plánuje ministr Bartoš. Aktuálně.cz. [Online] 1. 2 2022. [Citace: 25. 4 2022.]

https://zpravy.aktualne.cz/ekonomika/doprava/ridicak-uz-brzy-nebude-potreba-obcanka-postaci-elektronicka/r~f55d319e837011ec94760cc47ab5f122/.

ECHO MEDIA, a.s. © 2022. Podvodné SMS poslaly poslance ODS a TOP 09 do karantény. Echo24.cz. [Online] 2022. [Citace: 25. 4 2022.] https://echo24.cz/a/SJpY8/podvodne-sms-poslaly-poslance-ods-a-top-09-do-karanteny.

Elektronický podpis s.r.o. © 2022. Zaručený elektronický podpis. Elektronickypodpis.cz. [Online] 2022. [Citace: 25. 4 2022.] https://www.elektronickypodpis.cz/zaruceny-elektronicky-podpis/.

ESET software spol. s r.o. © 2022. Phishing. eset.com. [Online] 2022. [Citace: 30. 4 2022.] https://www.eset.com/cz/phishing/.

European Centre for Disease Prevention and Control (ECDC). © 2021. COVID-19 facts. EUROPEAN VACCINATION INFORMATION PORTALAn initiative of the European Union. [Online] 2021. [Citace: 29. 4 2022.] https://vaccination-info.eu/en/covid-19/covid-19-facts.

Gillis, Alexander S. © 2021. GUID (global unique identifier). techtarget.com. [Online] 2021. [Citace: 15. 4 2022.] https://www.techtarget.com/searchwindowsserver/definition/GUID-global-unique-identifier.

Hovorková, Kateřina. © 2020. Zrušení karenční doby nahrálo simulantům, tvrdí komora. Naopak, hájí ho Maláčová. Aktualne.cz. [Online] 28. 7 2020. [Citace: 25. 4 2022.] https://zpravy.aktualne.cz/ekonomika/spor-o-karencni-dobu-je-po-roce-zpet-firmy-trati-zamestnanci/r~eed8c6fccd9711eab408ac1f6b220ee8/.

Internet Info, s.r.o. © 2022. Ke službám eGovernmentu se už přihlásíte i pomocí svého účtu u služby MojeID. Lupa.cz. [Online] 2022. [Citace: 25. 4 2022.] https://www.lupa.cz/clanky/ke-sluzbam-egovernmentu-se-uz-prihlasite-i-pomoci-sveho-uctu-u-sluzby-mojeid/.

IT-Slovník.cz. © 2021. Co je to elektronizace? IT SLOVNÍK.cz. [Online] 2021. [Citace: 16. 12 2021.] https://it-slovnik.cz/pojem/elektronizace.

Katedra kybernetiky Západočeská univerzita v Plzni. © 2022. KYBERNETIKA. Katedra kybernetiky. [Online] 2022. [Citace: 29. 4 2022.] https://www.kky.zcu.cz/cs/definition-of-cybernetics.

Kluska, Vladislav. © 2020. Zprávy do datové schránky už nezmizí. Portál občana je umí zadarmo archivovat. Tuto funkci ale musíte zapnout. Živě.cz. [Online] 2020. [Citace: 25. 4 2022.] https://www.zive.cz/clanky/zpravy-do-datove-schranky-uz-nezmizi-portal-obcana-je-umi-zadarmo-archivovat-tuto-funkci-ale-musite-zapnout/sc-3-a-206630/default.aspx.

Krajská hygienická stanice Moravskoslezského kraje. © 2022, a. Důvod a způsob založení. khsova.cz. [Online] 2022, a. [Citace: 30. 4 2022.] https://www.khsova.cz/onas/povinne-informace106-zpusob.

Krajská hygienická stanice Moravskoslezského kraje. © 2022, b. Chřipka epidemie. KRAJSKÁ HYGIENICKÁ STANICE MORAVSKOSLEZSKÉHO KRAJE SE SÍDLEM V OSTRAVĚ. [Online] 2022, b. [Citace: 29. 4 2022.] https://www.khsova.cz/obcanum/otazky-chripka.

Lewik s.r.o. © 2021. Kybernetický prostor (zákon o kybernetické bezpečnosti, § 2). lewik.org. [Online] 2021. [Citace: 29. 4 2022.] https://www.lewik.org/term/13367/kyberneticky-prostor-zakon-o-kyberneticke-bezpecnosti-2/.

Magazín Egovernment. © 2022, a. NOVINKY V NÁRODNÍM IDENTITNÍM PROSTORU. Egovernment.cz. [Online] 2022, a. [Citace: 25. 4 2022.] https://www.egovernment.cz/inpage/nip/.

Magazín Egovernment. © 2022, b. PORTÁL PODNIKATELE MŮŽE BÝT K DISPOZICI JEŠTĚ LETOS, POKUD TO PŮJDE DOBŘE. Egovernment.cz. [Online] 2022, b. [Citace: 25. 4 2022.] https://www.egovernment.cz/inpage/portal-podnikatel/.

Machálková, Růžena. © 2021. Sabotáž a šikana hygieniků. Ministerstvo podá trestní oznámení na Landovo hnutí. Deník.cz. [Online] 12. 11 2021. [Citace: 25. 4 2022.] https://www.denik.cz/z_domova/trestni-oznameni-landa-zlaty-spendlik.html.

ManagementMania.com. © 2015. What-If Sensitivity Analysis. managementmania.com. [Online] 2015. [Citace: 30. 4 2022.] https://managementmania.com/en/what-if-analysis.

Medical Tribune. © 2013. Kde to drhne mezi praktiky a specialisty? Medical Tribune. [Online] 27. 5 2013. [Citace: 30. 4 2022.] https://www.tribune.cz/komentare/kde-to-drhne-mezi-praktiky-a-specialisty/.

Ministerstvo vnitra České republiky. © 2011. PROVOZNÍ ŘÁD INFORMAČNÍHO SYSTÉMU DATOVÝCH SCHRÁNEK. Ministerstvo vnitra České republiky. [Online] 10.

11 2011. [Citace: 16. 12 2021.] https://www.mvcr.cz/clanek/informacni-system-datovych-schranek-isds.aspx.

Ministerstvo vnitra České republiky. © 2021, a. APLIKAČNÍ PROGRAMOVÉ ROZHRANÍ (API) PRO PŘÍSTUP K CENTRÁLNÍM KOMPONENTÁM SYSTÉMU CZECHPOINT@OFFICE. Ministerstvo vnitra České republiky. [Online] 2021, a. [Citace: 16. 12 2021.] https://www.mvcr.cz/clanek/informacni-system-datovych-schranek-isds.aspx?q=Y2hudW09Mw%3d%3d.

Ministerstvo vnitra České republiky. © 2021, b. JEDNOTNÝ STANDARD PRO KOMUNIKACI MEZI SPISOVÝMI SLUŽBAMI (SS) A INFORMAČNÍM SYSTÉMEM DATOVÝCH SCHRÁNEK (ISDS). Ministerstvo vnitra České republiky. [Online] 2021, b. [Citace: 16. 12 2021.] https://www.mvcr.cz/clanek/informacni-system-datovych-schranek-isds.aspx?q=Y2hudW09Mg%3d%3d.

Ministerstvo vnitra České republiky. © 2021, c. Podpora elektronizace veřejné správy. Ministerstvo vnitra České republiky. [Online] 2021, c. [Citace: 16. 12 2021.] https://www.mvcr.cz/clanek/podpora-elektronizace-verejne-spravy.aspx.

Ministerstvo vnitra České republiky. © 2021, d. Základní registry a Správa základních registrů. Ministerstvo vnitra České republiky. [Online] 2021, d. [Citace: 16. 12 2021.] https://www.mvcr.cz/clanek/zakladni-registry-a-sprava-zakladnich-registru.aspx.

Ministerstvo vnitra České republiky. © 2022, a. Aplikační rozhraní. Datové schranky. [Online] 2022, a. [Citace: 25. 4 2022.] https://www.datoveschranky.info/technicke-pozadavky/aplikacni-rozhrani.

Ministerstvo vnitra České republiky. © 2022, b. Jaké služby poskytuje Czech POINT? Czech POINT. [Online] 2022, b. [Citace: 25. 4 2022.] https://www.czechpoint.cz/public/verejnost/sluzby/.

Ministerstvo vnitra České republiky. © 2022, c. Portál občana. gov.cz. [Online] 2022, c. [Citace: 25. 4 2022.] https://portal.gov.cz/caste-dotazy/portal-obcana.

Ministerstvo zdravotnictví. © 2020. Upozornění Ministerstva zdravotnictví k vystavování a vedení dočasné pracovní neschopnosti. mzcr.cz. [Online] 6. 1 2020. [Citace: 30. 4 2022.] https://www.mzcr.cz/upozorneni-ministerstva-zdravotnictvi-k-vystavovani-a-vedeni-docasne-pracovni-neschopnosti/.

Ministerstvo zdravotnictví. © 2021. Ministerstvo zdravotnictví. [Online] 2021. [Citace: 16. 12 2021.] https://www.mzcr.cz/druhy-zdravotni-pece/.

Ministerstvo zdravotnictví. © 2022. Jak funguje trasování? covid.gov.cz. [Online] 2022. [Citace: 15. 4 2022.] https://covid.gov.cz/situace/onemocneni-obecne-o-opatrenich/jak-funguje-trasovani.

Národní agentura pro komunikační a informační technologie. © 2021, a. Časté dotazy. Erouska.cz. [Online] 2021, a. [Citace: 25. 4 2022.] https://erouska.cz/caste-dotazy#obecne.

Národní agentura pro komunikační a informační technologie. © 2021, b. Chráním sebe, chráním tebe! Erouska.cz. [Online] 2021, b. [Citace: 25. 4 2022.] https://erouska.cz/.

Nejvyšší kontrolní úřad České republiky. © 2022. IT řešení pandemie: Stát připravený nebyl. Následné budování IT provázel chaos a improvizace. nku.cz. [Online] 25. 4 2022. [Citace: 30. 4 2022.] https://nku.cz/cz/pro-media/tiskove-zpravy/it-reseni-pandemie:-stat-pripraveny-nebyl--nasledne-budovani-it-provazel-chaos-a-improvizace-id12500/.

Němcová, Janetta. © 2020. Hygienické stanice se potýkají s nedostatkem lidí. Odborníky se nedaří najít i kvůli nízkým platům. irozhlas.cz. [Online] 11. 6 2020. [Citace: 25. 4 2022.] https://www.irozhlas.cz/zpravy-domov/zdravotnictvi-hygienicke-stanice-lekari-personalni-krize-koronavirus_2006110714_ada.

Odbor eGovernmentu. © 2015. Co je eGovernment? Ministerstvo vnitra České republiky. [Online] 25. 6 2015. [Citace: 16. 12 2021.] https://www.mvcr.cz/clanek/co-je-egovernment.aspx.

Rambousková, Michaela. © 2022. Vládní poslanci dostali falešné SMS o nástupu do karantény. seznamzpravy.cz. [Online] 2022. [Citace: 25. 4 2022.] https://www.seznamzpravy.cz/clanek/koronavirus-odpurci-pandemickeho-zakona-se-snazi-podvodem-poslat-poslance-do-karanteny-186978.

Reichl, Jiří. © 2021. Elektronizace veřejné správy bude pokračovat. Ministerstvo vnitra České republiky. [Online] 2021. [Citace: 16. 12 2021.] https://www.mvcr.cz/clanek/elektronizace-verejne-spravy-bude-pokracovat-116345.aspx.

Roche Czech Republic. © 2017. Pandemie infekčních onemocnění. mojemedicina.cz. [Online] 2017. [Citace: 29. 4 2022.] https://www.mojemedicina.cz/pruvodce-pacienta/diagnozy/pandemie-infekrnich-onemocneni.html.

Řehořek, Martin. © 2014. Problémy elektronizace zdravotnictví. computerworld.cz. [Online] 4. 3 2014. [Citace: 30. 4 2022.] https://www.computerworld.cz/clanky/problemy-elektronizace-zdravotnictvi/.

Solitea a.s. © 2021. Revoluce nebo evoluce? Jak bude od ledna 2020 fungovat elektronická neschopenka. money.cz. [Online] 2021. [Citace: 16. 12 2021.] https://money.cz/mzdy-a-personalistika/revoluce-evoluce-bude-od-ledna-2020-fungovat-elektronicka-neschopenka/.

Správa základních registrů. © 2022, a. Klíč k elektronickým službám. Identita občana. [Online] 2022, a. [Citace: 25. 4 2022.] https://www.identitaobcana.cz/Home/Citizen.

Správa základních registrů. © 2022, b. Klíč k elektronickým službám. identitaobcana.cz. [Online] 2022, b. [Citace: 25. 4 2022.] https://www.identitaobcana.cz/Home/Citizen.

Správa základních registrů. © 2022, c. REGISTR PRÁV A POVINNOSTÍ. Správa základních registrů. [Online] 2022, c. [Citace: 25. 4 2022.] https://www.szrcr.cz/cs/registr-prav-a-povinnosti.

Státní ústav pro kontrolu léčiv. © 2018. eRecept – oficiální stránky. epreskripce.cz. [Online] 2018. [Citace: 16. 12 2021.] https://www.epreskripce.cz/.

Státní ústav pro kontrolu léčiv. © 2022, a. Co je to opakovací recept a kdy je možné jej využít? Olecich.cz. [Online] 2022, a. [Citace: 30. 4 2022.] http://www.olecich.cz/encyklopedie/kdy-je-mozne-pouzit-opakovaci-recept.

Státní ústav pro kontrolu léčiv. © 2022, b. Portál Externích identit. pristupy.sukl.cz. [Online] 2022, b. [Citace: 29. 4 2022.] https://pristupy.sukl.cz/ei_forms.html.

Škorničková, Eva. © 2020. Informace o zdravotním stavu osob v době koronavirové. gdpr.cz. [Online] 24. 3 2020. [Citace: 30. 4 2022.] https://www.gdpr.cz/blog/informace-o-zdravotnim-stavu-osob-v-dobe-koronavirove/.

Štětina, Jiří. 2014. Zdravotnictví a integrovaný zachranný systém při hromadných neštěstích a katastrofách. Praha : Grada, 2014. ISBN 978-80-247-4578-7.

Ústav zdravotnických informací a statistiky ČR. © 2021. Pokyny ke kódování onemocnění COVID-19 (aktualizace). uzis.cz. [Online] 2021. [Citace: 30. 4 2022.] https://www.uzis.cz/index.php?pg=aktuality&aid=8379.

Ústav zdravotnických informací a statistiky ČR. © 2022, a. Informační systém infekční nemoci (ISIN). uzis.cz. [Online] 2022, a. [Citace: 29. 4 2022.]

https://www.uzis.cz/index.php?pg=registry-sber-dat--ochrana-verejneho-zdravi--informacni-system-infekcni-nemoci.

Ústav zdravotnických informací a statistiky ČR. © 2022, b. Národní registr zdravotnických pracovníků (NR-ZP). uzis.cz. [Online] 2022, b. [Citace: 29. 4 2022.] https://www.uzis.cz/index.php?pg=registry-sber-dat--narodni-registr-zdravotnickych-pracovniku.

Ústav zdravotnických informací a statistiky ČR. © 2022, c. Národní zdravotnický informační systém. Ústav zdravotnických informací a statistiky České republiky. [Online] 2022, c. [Citace: 25. 4 2022.] https://www.uzis.cz/index.php?pg=nzis.

Veřejná zdravotní pojišťovna. © 2021. Otázky týdne. Veřejná zdravotní pojišťovna České republiky. [Online] 2021. [Citace: 16. 12 2021.] https://www.vzp.cz/o-nas/tiskove-centrum/otazky-tydne/erecept-vs-papirovy-recept.

VPGC. © 2022. Top 5 kybernetických útoků zamířených na zdravotnictví. vpgc.com. [Online] 2022. [Citace: 25. 4 2022.] https://vpgc.com/top-5-kybernetickych-utoku-zamirenych-na-zdravotnictvi/.

vyhledatcislo.cz. © 2022. Telefonní číslo: 4636. vyhledatcislo.cz. [Online] 2022. [Citace: 30. 4 2022.] https://www.vyhledatcislo.cz/cislo/4636.

Whalebone. © 2021. Zdravotnictví pod kybernetickými útoky. whalebone.io. [Online] 8. 9 2021. [Citace: 25. 4 2022.] https://www.whalebone.io/post/zdravotnictvi-pod-kybernetickymi-utoky.

World Health Organization. © 2022. Coronavirus disease (COVID-19). World Health Organization. [Online] 2022. [Citace: 29. 4 2022.] https://www.who.int/health-topics/coronavirus#tab=tab_3.

# SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

SSL protokol zabezpečující komunikaci šifrováním a autentizaci komunikujících stran

GUID jedinečný celosvětový identifikátor hardwaru, softwaru, účtů, dokumentů atp.

RFC očíslované doporučené specifikace popisující internetové protokoly a systémy

SMS v textu jsou tak označeny krátké textové zprávy posílané mezi mobilními telefony

ČR Česká republika

# SEZNAM OBRÁZKŮ

Obrázek 1 mapa Czech POINT (Ministerstvo vnitra České republiky, © 2022, b) ..... 15
Obrázek 2 karanténa a trasování ..... 57
Obrázek 3 blokované zprávy a marketingové nabídky ..... 59
Obrázek 4 duplicitní zprávy KHS ..... 60

# SEZNAM TABULEK

Tabulka 1 Četnost rizika Ilustrační (APTIEN.COM, © 2021) ..... 27
Tabulka 2 Úroveň rizika Ilustrační (APTIEN.COM, © 2021) ..... 27
Tabulka 3 Celková míra rizika (APTIEN.COM, © 2021) ..... 28
Tabulka 4 Četnosti rizika ..... 47
Tabulka 5 Úroveň rizika ..... 48
Tabulka 3 Celková míra rizika (APTIEN.COM, © 2021) ..... 48
Tabulka 6 Metoda What if s maticí rizik ..... 49