Ministerstvo zdravotnictví České republiky
Palackého nám. č 4, 128 01 Praha 2, IČ: 00024341

Verze: v1.0
Platnost nové verze od:
03.08.2021
Spisový znak: 05.02.2108
Skartační znak a lhůta: V/5

Strategie kybernetické bezpečnosti resortu zdravotnictví 2021-2025

Pořadí revize	Provedené dne	Zpracoval	Schválil
1.0	29.6 2021	Tomáš Bezouška manažer kybernetické bezpečnosti	Martin Zeman předseda výboru pro řízení kybernetické bezpečnosti

Obsah

Seznam tabulek

Seznam zkratek a pojmů

Zkratka	Význam
ENISA	Agentura Evropské unie pro kybernetickou bezpečnost (The European Union Agency for Cybersecurity)
ICT (IKT)	Information and Communication Technology (Informační a komunikační technologie)
IDRR	Projekt „Informační a datové resortní rozhraní“, infrastrukturní komponenta pro realizaci dalších projektů Národní strategie elektronického zdravotnictví
IPVZ	Institut postgraduálního vzdělávání ve zdravotnictví
JTP	Jednotná technologická platforma (soubor informačních technologií tvořící technický základ pro provoz významných informačních systémů resortu, určený jako KII)
KB	Kybernetická bezpečnost
KII	Kritická informační infrastruktura, definovaná v ZKB
Kybernetická bezpečnost	Soubor organizačních a technických opatření, zajišťujících ochranu důvěrnosti, dostupnosti a integrity u vybraných aktiv organizace. Informační a kybernetická bezpečnost jsou použity jako synonymum v kontextu tohoto dokumentu.
MZČR	Ministerstvo zdravotnictví ČR
NCEZ	Národní centrum elektronického zdravotnictví
PZS	Provozovatel základní služby ve smyslu § 2 písm. k) ZKB
SIEM	Nástroj pro řízení bezpečnostních informací a událostí (Security Information and Event Management)
SOC	Operační centrum informační bezpečnosti (Security Operations Center)
SÚKL	Státní ústav pro kontrolu léčiv
ÚZIS	Ústav zdravotnických informací a statistiky ČR
VIS	Významný informační systém, definován v ZKB
VKB	Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
ZKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

Tabulka 1 Seznam zkratek a pojmů

1 Úvod

Strategie kybernetické bezpečnosti resortu zdravotnictví pro roky 2021-2025 představuje vrcholový dokument ukotvující snahy a aktivity Ministerstva zdravotnictví České republiky a dalších systémových aktérů, jako je Národní úřad pro kybernetickou a informační bezpečnost, Ústav zdravotnických informací a statistiky a další, směřující ke zvýšení kybernetické bezpečnost napříč sektorem zdravotnictví. Strategie navazuje na obdobný dokument formulovaný pro roky 2015-2020, přičemž ale dochází k zásadnímu rozšíření záběru dokumentu a strategického fokusu z organizací a systémů přímo dotčených zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, na všechny organizace a cílové skupiny působící v rámci resortu.

Oblast zdravotnictví se stává stále významnějším cílem kybernetických útoků, stupňuje se jejich četnost, míra sofistikovanosti a potenciál poškodit primární účel napadených organizací – poskytování zdravotních služeb. Cílem této strategie je tak především posilování systémové odolnosti resortu zdravotnictví a jeho jednotlivých organizací, a to ve všech oblastech relevantních pro zvýšení kybernetické bezpečnosti, od zavádění systémů řízení bezpečnosti informací, přes posilování technických prostředků kybernetické bezpečnosti až po vzdělávání.

Samostatnou skupinu problémů, kterými se strategie zabývá a jejichž řešení by měla umožnit, je zajištění financování pro naplňování jednotlivých strategických cílů. V rámci strategického období je možné čerpat významné prostředky zejména z finančních instrumentů Evropské unie a příprava absorpční kapacity spolu s vytvářením strategického rámce pro efektivní uplatnění těchto zdrojů je tak jedním ze zásadních fokusů strategie.

Strategie je formulována s přihlédnutím k dalším strategickým dokumentům jak v oblasti kybernetické bezpečnosti, tak digitalizace veřejné sféry. Klíčovými zdroji jsou v tomto ohledu zejména následující dokumenty:

- Národní strategie kybernetické bezpečnosti České republiky na období let 2021–2025
- Program Digitální Česko Informační koncepce ČR
- Schválená Národní strategie elektronického zdravotnictví na období 2016–2020
- The EU's Cybersecurity Strategy for the Digital Decade

1.1 Cíle a účel dokumentu

Kybernetická bezpečnost se přirozeně stává společníkem našich každodenních činností, oblast zdravotnictví nevyjímaje. S rozmachem elektronizace informací a jejich zpracovávání čelíme i novým výzvám v podobě nových technologií a přístupů ke sdílení dat a informací. V této oblasti pak pochopitelně zdravotní údaje patří k datům nejcitlivějším.

Tento dokument si klade za cíl stanovit jak rámec, tak jednotlivé kroky v podobě hierarchické struktury cílů pro dosažení optimálního nastavení ochrany informací

napříč resortem Ministerstva zdravotnictví České republiky. Tyto dílčí kroky v podobě cílů doplňují záměr zavedení a rozvoje procesů elektronického zdravotnictví České republiky na období let 2021–2025

Smyslem tohoto strategického dokumentu je vymezení základní vize v oblasti kybernetické bezpečnosti a v návaznosti na tuto vizi stanovení strategických cílů a konkrétních programů a projektů vedoucích k její realizaci. Strategie bude procházet každoroční evaluací, v jejímž rámci bude vyhodnocen pokrok v naplňování strategických cílů, případné změny v okolním prostředí a jejich dopad do vize a definovaných strategických cílů, včetně zpracování akčního plánu na následující období.

Strategie kybernetické bezpečnosti resortu Ministerstva zdravotnictví České republiky, stejně jako výroční zprávy o jejím naplňování a její případné revize, bude po projednání Výborem pro řízení kybernetické bezpečnosti resortu předložena ke schválení poradě vedení ministerstva pro období 2021-2025.

1.2 Závaznost dokumentu a vymezení kompetencí

Tento dokument představuje strategickou vizi pro kybernetickou bezpečnost resortu Ministerstva zdravotnictví. Po formální stránce se jedná o interní dokument ministerstva a jeho závěry nejsou právně závazné pro žádnou z organizací, které jsou v dokumentu ať už přímo či nepřímo zmíněny. Dokument slouží jako deklarace politiky Ministerstva zdravotnictví ČR pro oblast kybernetické bezpečnosti s cílem přispět k bezproblémovému fungování jak jednotlivých organizací, tak resortu zdravotnictví jako celku.

Na poli kybernetické bezpečnosti je vrcholným orgánem státní správy Národní úřad pro kybernetickou a informační bezpečnost. Ministerstvo zdravotnictví nemá ambici tímto dokumentem ani dalšími aktivitami v oblasti kybernetické bezpečnosti zasahovat do jeho kompetencí, naopak je smyslem dokumentu přispět ke zvyšování kybernetické bezpečnosti napříč resortem zejména u organizací, které z definice dané zákonem dosud nespadají do přímé gesce NÚKIB a nalézat vzájemné synergie mezi aktivitami obou úřadů v této oblasti tak, aby byla posílena kybernetická bezpečnost, pokud možno všech organizací resortu zdravotnictví.

Ministerstvo zdravotnictví a tato strategie plně respektují přímou kompetenci NÚKIB ve vztahu k orgánům a osobám, kterým jsou ukládány povinnosti v oblasti kybernetické bezpečnosti zákonem. Pokud by jakákoliv část této strategie a navazujících dokumentů připouštěla jiný výklad, vždy bude přednostně uplatněn tento základní princip.

Organizace, uváděné v rámci soustavy cílů ať už jako „Klíčoví aktéři“, nebo jako „Zdroje“, nejsou touto strategií vázáni k zajištění konkrétních činností či projektů a jejich spolupráce bude vždy vyplývat ze vzájemné diskuse, případně v rámci dělení kompetencí státní správy vyplývá z jejich role ve státním aparátu a bude komunikována standardními cestami.

2 Vyhodnocení Strategie KB MZČR 2016-2020

Strategie kybernetické bezpečnosti v období 2016–2020 obsahovala strukturu strategických a specifických cílů, zaměřených především na etablování strukturovaného přístupu ke kybernetické bezpečnosti v rámci organizací přímo dotčených zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, na rozvoj povědomí o otázkách informační a kybernetické bezpečnosti v organizacích resortu a na začlenění principů kybernetické bezpečnosti jako nedílné součástí rozvoje elektronického zdravotnictví.

Následující kapitola shrnuje v přehledné podobě stav jednotlivých cílů ze Strategie kybernetické bezpečnosti MZČR 2016-2020, včetně stručného komentáře k průběhu či výsledkům plnění daného cíle.

2.1 SC1 Zavedení resortního systému řízení kybernetické bezpečnosti

Specifický cíl	Stav	Komentář
Vytvořit efektivní model spolupráce na resortní úrovni mezi jednotlivými dotčenými organizacemi v resortu MZ ČR a subjekty kybernetické bezpečnosti.	Splněna 1. etapa	• Pro organizace podřízené ZKB vytvořena Rada bezpečnostních rolí a Výbor pro řízení kybernetické bezpečnosti s koordinační rolí • V druhé etapě bude model spolupráce rozšířen, aby byly naplněny konkrétní potřeby organizací resortu. • Vzorové metodiky KB publikovány pro potřeby organizací resortu MZČR
Zajistit efektivitu a posilování všech struktur, procesů a spolupráce při zajišťování kybernetické bezpečnosti.	Splněno	• Pro organizace podřízené ZKB vytvořena Rada bezpečnostních rolí a Výbor pro řízení kybernetické bezpečnosti s koordinační rolí • Vzorové metodiky KB publikovány pro potřeby organizací resortu MZČR
Vybudovat resortní SOC sloužícího k monitoringu KII a VIS resortu, vyhodnocování bezpečnostních hrozeb a incidentů	V řešení	• Řešeno Ústavem zdravotnických informací a statistiky ČR • Centrální SOC je řešen jako služba k využití dle dispozic jednotlivých PZS.

Specifický cíl	Stav	Komentář
Vytvořit resortní, koordinovaný postup pro zvládání incidentů, který nastaví formát spolupráce, bude obsahovat komunikační matici, protokol postupu a definovat jednotlivé role aktérů.	V řešení	• Metodika řízení kybernetických událostí a incidentů organizací v přímé působnosti MZČR je připravena k projednání Radou a Výborem
Vytvořit metodologii pro hodnocení rizik na úrovni dotčených organizací v resortu MZ ČR.	Splněno	• Součást metodik KB vydávaných MZČR
Udržovat jednotný postoj resortu MZ ČR směrem do zahraničí, který bude koordinován s ostatními resorty zainteresovanými v oblasti kybernetické bezpečnosti.	Probíhá	• Zapojení v ENISA • Aktivity NCEZ v rámci eHealth Network
Zohledňovat odpovídajícím způsobem neustále se vyvíjející problematiku kybernetických hrozeb v rámci tvorby a aktualizací významných bezpečnostně strategických materiálů MZ ČR, České republiky (Bezpečnostní strategie České republiky a další).	Probíhá	• Spolupráce s NÚKIB na revizi Strategie KB ČR • Aktualizace metodik KB vydávaných MZČR dle novelizace VKB

2.2 SC2 Ochrana resortní KII a VIS

Specifický cíl	Stav	Komentář
Pokračovat v průběžné analýze a kontinuálním sledování zabezpečení systémů KII a VIS v resortu MZ ČR pomocí jasně definovaných metodik.	Probíhá	• Nastaven proces • Probíhající aktivita v rámci dokumentace KB MZČR/ÚZIS a projektu IDRR
Průběžně navyšovat odolnost, integritu a	V řešení	• Probíhá v rámci jednotlivých projektů v působnosti ÚZIS ČR

Specifický cíl	Stav	Komentář
důvěryhodnost systémů a sítí KII a VIS.		
Kontinuálně provádět analýzu a monitoring hrozeb a rizik v dotčených organizací v resortu MZ ČR, případně v širším kontextu resortu MZ ČR.	V řešení	• Analýza rizik KII a VIS byla provedena • Analýza hrozeb ostatních organizací a systémů (zejména PSZ) je prováděna organizacemi samostatně. Bude vyhodnocována v rámci projektu KB MZ • Kontinuální monitoring (SIEM) Zavedl ÚZIS ČR na KII/VIS infrastruktuře a provozní infrastruktuře MZČR/ÚZIS ČR a několika organizacích, nikoli na centrální úrovni
Efektivně sdílet informace mezi NÚKIB, resortním SOC a dotčenými organizacemi v resortu MZ ČR.	Splnění podmíněno	• Resortní SOC není dosud zaveden • Nejsou dobudovány další SOC v resortu zdravotnictví
Navyšovat technologické kapacity a schopnosti resortního SOC a v rovině personální neustále vzdělávat a školit zaměstnance/experty tohoto pracoviště.	Splnění podmíněno	• Resortní SOC není dosud zaveden
Důkladně a důvěryhodně zabezpečit prostředí pro skladování a práci s daty subjektů KII a VIS, které zřídí a bude spravovat MZ ČR.	Splněno částečně	• Důvěryhodné úložiště zabezpečuje ÚZIS • Práce s daty dosud není v zavedena v působnosti MZ
Pravidelně provádět kontroly a zajišťovat odhalování chyb a zranitelností v informačních systémech a sítích využívaných v dotčených organizací v resortu MZ ČR, založené na principu penetračních testů.	Splněno částečně	• Penetrační testy JTP realizoval ÚZIS • Penetrační testy VIS SÚKL realizoval SÚKL • MZČR ve spolupráci s ÚZIS připravuje veřejnou zakázku na penetrační testování pro organizace v resortu na principu centrálního zadávání.

Specifický cíl	Stav	Komentář
Průběžně navyšovat technologické a organizační předpoklady k aktivnímu odvrácení (potlačení) kybernetických útoků.	Řešeno průběžně	• ÚZIS zajišťuje technické předpoklady a provoz pro infrastrukturu KII, VIS a vybrané přímo řízené organizace MZČR • NCEZ – příprava programu podpory řešení KB u PZS a realizace konkrétních projektů
Zvyšovat resortní možnosti, schopnosti a kapacity v oblasti aktivní obrany a protiopatření proti kybernetickým útokům.	V řešení	• NCEZ – příprava programu podpory řešení KB u PZS a realizace konkrétních projektů
Vzdělávat specializované odborníky, kteří se zaměří na problematiku a možnosti aktivních protiopatření při zajišťování kybernetické bezpečnosti a obrany a na obecně ofenzivní pojetí kybernetické bezpečnosti.	Splněno částečně	• NCEZ – příprava programu podpory řešení KB u PZS a realizace konkrétních projektů
Zpracovat postup pro přechod mezi vyhlášeným stavem kybernetického nebezpečí dle zákona o kybernetické bezpečnosti a stavy dle ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky.	Nesplněno	• NCEZ – příprava programu podpory řešení KB u PZS a realizace konkrétních projektů

2.3 SC3 Vzdělávání a osvěta v oblasti kybernetické bezpečnosti

Specifický cíl	Stav	Komentář
Navyšovat povědomí a gramotnost v otázkách kybernetické bezpečnosti u odborné veřejnosti v rámci resortu Ministerstva zdravotnictví, pomocí podpory iniciativ a	V řešení	• Poskytnuty podklady pro základní školení KB • Provedena řada školení pro zdravotnickou veřejnost ve spolupráci s IPVZ

Specifický cíl	Stav	Komentář
osvětových kampaní, pořádáním konferencí pro odbornou veřejnost apod.		• Zahájena spolupráce s NÚKIB na poskytnutí eLearningu zaměřeného na KB ve zdravotnických zařízeních
Vzdělávat a školit zaměstnance dotčených organizací v resortu MZ ČR působící zejména v oblasti kybernetické bezpečnosti a informační kriminality.	Plněno průběžně	• Organizacím resortu poskytnuty podklady pro základní školení KB • Provedena řada školení pro zdravotnickou veřejnost ve spolupráci s IPVZ • Realizována školení pro zaměstnance MZČR a ÚZIS

2.4 SC4 Resortní předpisy pro kybernetickou bezpečnost

Specifický cíl	Stav	Komentář
Podílet se na tvorbě a implementaci národních, evropských a mezinárodních pravidel.	Plněno průběžně	• Spolupráce s NÚKIB • Zapojení v ENISA • Aktivity v rámci eHealth Network
Na základě systematického přístupu, tj. vzhledem k existujícím právním předpisům, vytvářet v oblasti kybernetické bezpečnosti srozumitelné, efektivní a proporcionální resortní předpisy.	V řešení	• Příprava zákona o elektronickém zdravotnictví probíhá a aspekty kybernetické bezpečnosti jsou zohledňovány • Probíhá zařazení nemocnic mezi poskytovatele základní služby dle vyhlášky č. 82/2018 Sb.
Aktivně se účastnit na tvorbě a implementaci národních, evropských a mezinárodních pravidel.	V řešení	• Zapojení v ENISA • Aktivity v rámci eHealth Network
Zpracovat metodiku implementace kybernetické bezpečnosti pro zdravotnická zařízení a propagovat aktuální znění metodiky formou seminářů, školení jak po jejím vytvoření, tak v případě větších novelizací.	Plněno průběžně	• Metodika zveřejněna • Informace o metodice publikovány na dostupných fórech • Aktivita bude průběžně pokračovat pod řízením NCEZ
Provádět jak kontinuální analýzu efektivity účinné	V řešení	• Probíhá v součinnosti s NÚKIB

Specifický cíl	Stav	Komentář
právní úpravy a jejího souladu s aktuálními poznatky z dotčených technických a společenskovědních oborů, tak i průběžné provádění změn a doplňování tak, aby resortní úprava odpovídala aktuálním požadavkům bezpečné informační společnosti.		• V rámci strategického období došlo k rozšíření působnosti kybernetického zákona na poskytovatele základní služby a po vyhodnocení právní úpravy o další rozšíření množiny organizací spadajících do této kategorie • Jsou diskutovány minimální standardy kybernetické bezpečnosti a další opatření • Specifický cíl má kontinuální, resp. cyklickou povahu (PDCA) a je přenesen i do dalšího strategického období

2.5 SC5 Elektronizace zdravotnictví a implementace kybernetické bezpečnosti

Specifický cíl	Stav	Komentář
Aktivně se účastnit na tvorbě a implementaci nových pravidel pro elektronizaci zdravotnictví a práci s dokumenty v digitální podobě v oblasti zdravotnické dokumentace a ve zdravotnictví obecně a promítat do ní principy kybernetické bezpečnosti.	V řešení	• Zapracování pravidel do zákona o elektronickém zdravotnictví a zákona o zdravotních službách. Aspekty kybernetické bezpečnosti jsou zohledňovány.

2.6 Shrnutí

Významnou část stanovených cílů ze strategie 2016–2020 se podařilo v daném obdobní naplnit, anebo – zejména v případě dlouhodobých investičních akcí – alespoň zahájit jejich plnění. Současně došlo v průběhu strategického období k zásadnímu posunu, kterým bylo zavedení kategorie poskytovatelů základní služby do zákona o kybernetické bezpečnosti.

Tento krok přinesl celou řadu dalších úkolů souvisejících s touto koncepční změnou, které se podařilo do značné míry realizovat, ať už to bylo zajištění financování rozvoje kybernetické bezpečnosti pro významnou část dotčených zdravotnických zařízení, nebo nastartování metodické podpory jak z úrovně

Ministerstva zdravotnictví a ÚZIS, tak ve spolupráci s Národním úřadem pro kybernetickou a informační bezpečnost.

Úkoly a problémy, které se v uplynulém strategickém období nepodařilo dokončit, jsou v podstatné části přeneseny do struktury cílů v novém strategickém období a spoluvytvářejí tak kontinuitu aktivit v oblasti rozvoje kybernetické bezpečnosti.

3 Analýza

3.1 Analýza současného stavu

Celý resort zdravotnictví, stejně jako jednotlivé organizace, čelí novým výzvám, souvisejícím s poskytováním a udržováním spolehlivých služeb v rychle se vyvíjejícím technologickém prostředí. Čím dál tím větší část činností a procesů prováděna a dodávána za významné podpory informačních technologií a zapojení moderních informačních technologií je také ve stále větší míře vyžadováno klienty zdravotních služeb – pacienty a občany. V důsledku toho se data a informace stávají velmi důležitými aktivy nehledě na charakter organizace a její postavení v sektoru zdravotnictví.

V souladu s výše uvedeným je zásadním požadavkem zajistit správu těchto informačních aktiv způsobem, který bude trvale garantovat jejich zpřístupnění (dostupnost) řádně oprávněným osobám (důvěrnost) a zajistí jejich úplnost, pravdivost a kvalitu (integrita). Takto pojatá bezpečnost informací se stává klíčovým předpokladem zajištění resilience jednotlivých poskytovatelů zdravotních služeb i celého sektoru.

V posledních letech dochází k opakovanému plošnému nárůstu kybernetických útoků, a oblast zdravotnictví je jedním z jejich prominentních cílů. Podle zprávy jedné ze společností zabývající se kybernetickou bezpečností, je zřejmé, že jen v listopadu a prosinci 2020 došlo celosvětově k 45 % nárůstu kybernetických útoků na zdravotnické organizace. Tento nárůst je více než dvojnásobný ve srovnání se všemi průmyslovými odvětvími ve stejném období. Celosvětově došlo v listopadu a prosinci 2020 v průměru ke 626 kybernetickým útokům na zdravotnické organizace, oproti 430 útokům v říjnu. (zdroj: ZDE).

Další společnost se zaměřením na kybernetickou bezpečnost uvedla, že z jejich statistik vyplývá, že v roce 2017 bylo ransomware infikováno 30 % počítačů a zařízení využívaných ve zdravotnických organizacích. Tento počet ale neustále klesá, v roce 2018 to bylo 28 %, loni (2019) dokonce už jen 19 %. (zdroj: ZDE)

V České republice byly mediálně diskutovány zejména případy kybernetického útoku na Nemocnici Rudolfa a Stefanie v Benešově, Fakultní nemocnici Brno a Psychiatrickou nemocnici Kosmonosy. Škody způsobené těmito útoky jsou popsány v tabulce níže. V důsledku kybernetických útoků musela jednotlivá zdravotnická zařízení zastavit nebo výrazně omezit poskytování zdravotních služeb, a to i na dobu několika týdnů, protože byla jejich zdravotnická data odcizena, zašifrována nebo mohla být modifikována.

Název organizace	Datum útoku	Odhadovaná škoda v souvislosti s útokem
Nemocnici Rudolfa a Stefanie Benešov	Prosinec 2019	<59 000 000 Kč
Fakultní nemocnice Brno	Březen 2020	<100 000 000 Kč
Psychiatrická nemocnice Kosmonosy	Březen 2020	n/a

Tabulka 2 Největší kybernetické útoky na zdravotnická zařízení v ČR

Kybernetické bezpečnostní incidenty jsou ve zdravotnictví často výsledkem souběhu několika faktorů. Na jedné straně technologické faktory, což mohou být zastaralé a složité systémy IT, které jsou klíčové pro organizace a které jsou citlivé na kybernetické útoky a selhání. Na druhé straně organizační faktory, jako značný nedostatek povědomí a školení odborníků v oblasti bezpečnosti informací, otázek, trendů a rizik v oblasti kybernetické bezpečnosti.

Důsledkem útoku mohou být škody na zdraví a životech, ať už v důsledku nutnosti odložit akutní péči, nebo v důsledku nenávratné ztráty dat či např. poškození jejich integrity. Kybernetické útoky, kromě finančních ztrát a zhoršování reputace zasažené instituce, také významně snižují důvěru klientů v nakládání s jejich zdravotnickou dokumentací a osobními údaji.

Spolu s nárůstem navzájem propojených systémů a zařízení, následně s potřebou výměny dat na národní i mezinárodní úrovni, se zvyšují rizika s dopadem na integritu a důvěrnost dat a vyžadují pozornost možných narušení komunikací a IT systémů. Pouze se správnými bezpečnostními strategiemi mohou zdravotnické organizace zajistit, aby byla citlivá data adekvátně chráněna, identifikující zranitelná místa a potenciální místa vstupu dat a informací do nemocnic a systémů jiných zdravotnických zařízení. Zabezpečení informací a zdravotnických dat o pacientech, je ve skutečnosti jednou z největších výzev, jimž sektor zdravotnictví čelí uvnitř i vně organizace při elektronické výměně dat mezi organizacemi (nemocnicemi a dalšími zdravotnickými zařízeními).

Zdravotnické organizace stále čelí největším rizikům a dopadům v případě kybernetického incidentu v porovnání s ostatními odvětvími, vzhledem k tomu, že následkem neposkytnutí zdravotních úkonů vlivem kybernetického bezpečnostního incidentu, může dojít až ke ztrátám na životech, či vážným zdravotním komplikacím. Obecně řečeno, všechny zdravotnické organizace by měly chápat rizika prostřednictvím dobře definovaných a dobře řízených iniciativ v oblasti kybernetické bezpečnosti, poskytujících holistickou vizi spojenou do jediného integrovaného rámce a zastřešující strategii zahrnující procesy, lidi a technologie organizace, aby zajistily efektivní a účinnou ochranu dat a informací.

Proto je nutné zaměřit pozornost na soubor procesů, lidí a technologií, které zajišťují odolnější a bezpečnější poskytování zdravotní péče, což vede ke snížení rizika důvěrnosti, integrity a dostupnosti zdravotních informací a zvýšení důvěry pacientů v technologie zpracovávající zdravotnická data.

Analýza současného stavu reflektuje aktuální stav prostředí zdravotnictví České republiky. Při zpracování této analýzy bylo přihlédnuto zejména k povinnostem stanoveným aktuálně platnými zákony. Bylo také přihlédnuto k dalším strategickým dokumentům pokrývajícím dlouhodobé rozvojové záměry České republiky v oblasti digitalizace, mezinárodní doporučení v oblasti eHealth (elektronického zdravotnictví) a v neposlední řadě také reakcím respondentů z řad organizací, poskytujících zdravotní služby a další související služby navázané na systém poskytování zdravotní péče v České republice.

Události z konce roku 2019 a začátku roku 2020 poukázaly na význam kybernetické a informační bezpečnosti nejen pro subjekty přímo podřízené ZKB, ale pro všechny organizace v resortu Ministerstva zdravotnictví České republiky, a na **nutnost posílení systémového řešení** celé problematiky, stejně jako zajištění dostatečných finančních zdrojů a odborných kapacit k významnému posílení kybernetické bezpečnosti českého zdravotnictví jako celku i každé jednotlivé organizace.

Součástí cílů pro nadcházející období let 2021-2025 je mimo jiné také potřeba poskytovat ze strany MZČR metodickou podpory všem organizacím resortu Ministerstva zdravotnictví České republiky. Tato metodická podpora je zaměřená především na zvyšování bezpečnostního povědomí a metodickou pomoc při zavádění systémů řízení bezpečnosti informací, reflektujících principy uplatněné v ZKB a jeho prováděcích vyhláškách, ve všech organizacích zapojených do systému poskytování zdravotní péče.

Výsledky interního průzkumu MZČR

Byl proveden průzkum stavu kybernetické bezpečnosti, v rámci kterého bylo osloveno 279 poskytovatelů zdravotních služeb. Od 163 organizací, které odpověděli na 145 otázek byla získána důležitá data a informace, která mimo jiné pomáhala formovat a utvářet směr vývoje kybernetické bezpečnosti resortu zdravotnictví České republiky.

Z odpovědí zdravotnických zařízení, které byly shromážděny v rámci průzkumu v oblasti kybernetické bezpečnosti vyplývá, že téměř 60 % dotazovaných organizací nemá zaveden systém řízení bezpečnosti informací. Zavedení systému řízení bezpečnosti informací je základním předpokladem pro zajištění efektivní ochrany klíčových procesů jakékoliv organizace. Dále z uvedeného průzkumu vyplývá, že penetračnímu testování se pravidelně nevěnují ani ty největší zdravotnické organizace, kde by se dalo předpokládat, že disponují dostatečným personálním i dalším zajištěním pro provádění tohoto základního testování na výskyt zranitelností v ICT prostředí organizace. 86 % respondentů uvedlo, že určování dopadů na kybernetickou bezpečnost není součástí

posuzování nemocničních přístrojů, a to i přes to, že 46 % respondentů nemá tyto přístroje v separátní LAN síti.

Identifikace zdrojů dat a zpracování primárních analýz

Při zpracování analýzy bylo vycházeno z těchto dokumentů:

Název dokumentu	Revize/verze	Ze dne
Akční plán pro oblast kybernetické bezpečnosti resortu MZ ČR	2	25. 9. 2017
Program Digitální Česko Informační koncepce ČR	Finální	20.9.2018
Strategie kybernetické bezpečnosti resortu MZ ČR	2.01	27.3.2019
Program Digitální Česko Digitální ekonomika a společnost	Finální	20.9.2018
Informace o stavu aktualizace Strategie kybernetické bezpečnosti resortu MZČR a přípravě strategického rámce v oblasti kybernetické bezpečnosti pro roky 2021-2025	Neuvedeno	Srpen 2020
Program Digitální Česko Zpráva o plnění programu Digitální Česko	Finální	3.10.2018
Dotazník pokrývající oblast kybernetické bezpečnosti pro nemocnice	Finální	29.7.2020
Common security framework for eHealth systems and services at a national and at a cross-border level	0.12	26.2.2020
Směrnice rady 2008/114/ES, ze dne 8. prosince 2008, o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu.	Finální	8.12.2008
Průzkum zdravotnických zařízení v oblasti kybernetické bezpečnosti.	Finální	Q1 2020
Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020 https://nukib.cz/cs/infoservis/dokumenty-a-publikace/strategie-akcni-plan/	Finální	16.2.2015
Národní strategie kybernetické bezpečnosti České republiky na období let 2021–2025	Finální	2.12.2020

Název dokumentu	Revize/verze	Ze dne
https://nukib.cz/cs/infoservis/dokumenty-a-publikace/strategie-akcni-plan/		
Vize elektronického zdravotnictví ČR https://ncez.mzcr.cz/cs/dokumenty/vize-elektronickeho-zdravotnictvi-cr	Finální	18.1.2015
Schválená Národní strategie elektronického zdravotnictví na období 2016–2020 https://ncez.mzcr.cz/cs/dokumenty/schvalena-narodni-strategie-elektronickeho-zdravotnictvi-na-obdobi-2016-2020	Finální	11.10.2016
Procurement Guidelines for Cybersecurity in Hospitals https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services	Finální	24.2.2020
STATE OF CYBERSECURITY & CYBER THREATS IN HEALTHCARE ORGANIZATIONS (2017) https://blogs.harvard.edu/cybersecurity/files/2017/01/risks-and-threats-healthcare-strategic-report.pdf	Finální	28.6.2016
MOVING FORWARD FOR CYBERSAFE HEALTHCARE: INSIGHTS FROM THE CANADIAN SUMMIT ON HEALTHCARE CYBERSECURITY (2018) https://www.healthcarecan.ca/2018/09/10/moving-forward-for-cybersafe-healthcare-insights-from-the-canadian-summit-on-healthcare-cybersecurity/	Finální	22.8.2018
JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL – The EU's Cybersecurity Strategy for the Digital Decade https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020JC0018	Finální	16.12.2020

Z těchto dokumentů byly čerpány nejen požadavky na uspořádání, funkcionalitu a architekturu, ale i dlouhodobé záměry a strategie, cíle a úkoly pro vytvoření prostředí s odpovídající a udržitelnou úrovní zabezpečení. Tato úroveň zabezpečení nejen musí reflektovat aktuální požadavky, ale zejména podporovat dynamicky se rozvíjející požadavky na modernizaci v poskytování

zdravotnické péče, požadavky na sdílení informací a v neposlední řadě také procesování dat a informací v reálném čase.

Analýza dosavadních řešení včetně mezinárodní praxe

Z dokumentu Strategie kybernetické bezpečnosti EU pro digitální dekádu vyplývá, že obavy o bezpečnost jsou velkou překážkou používání on-line služeb. Přibližně dvě pětiny uživatelů v EU zažily problémy související s bezpečností a tři pětiny mají dojem, že se nedokážou chránit před kyberkriminalitou. Třetina uživatelů se za poslední tři roky setkala s podvodnými e-maily nebo telefonními hovory žádajícími o osobní údaje, 83 % z nich však kyberkriminalitu nikdy nenahlásilo. Každý osmý podnik byl zasažen kybernetickými útoky. Více než polovina podnikových a spotřebitelských osobních počítačů, které jsou jednou infikovány malwarem, je opakovaně infikována ve stejném roce. Každý rok se z důvodu porušení zabezpečení dat ztratí stovky milionů záznamů; průměrné náklady při narušení zabezpečení u jednoho podniku vzrostly v roce 2018 na více než 3,5 milionu EUR. Dopad kybernetického útoku často nelze izolovat a jeho důsledkem mohou být řetězové reakce v celé ekonomice a společnosti, které ovlivní miliony jednotlivců.

Kybernetická bezpečnost je nepostradatelná pro síťovou konektivitu a globální a otevřený internet, které musí podpořit transformaci ekonomiky a společnosti ve 20. letech 21. století. Přispívá k lepším dovednostem a většímu počtu pracovních míst, flexibilnějším pracovištím, efektivnějším a udržitelnějším odvětvím dopravy a zemědělství a snadnějšímu a spravedlivějšímu přístupu ke zdravotnickým službám.

K nežádoucím událostem z hlediska kybernetické bezpečnosti dochází v každé organizaci a nikdy je nebude možno zcela eliminovat. Prostřednictvím důrazu na kvalitu a bezpečnost je ale možné je minimalizovat a mnoha z nich předcházet. Zatímco dosud organizace k problematice přistupovaly tak, že měřily nežádoucí události a z toho vyvozovaly bezpečnost, novým trendem je snažit se už dopředu na základě zkušeností vlastních i cizích proaktivně rizika minimalizovat.

Rámec pro nastavení efektivního a udržitelného způsobu ochrany informací a dat je založen na požadavcích ZKB, prostřednictvím jeho prováděcích vyhlášek VKB. Oba dokumenty identifikují osoby povinné dle ZKB, organizační a technická opatření pro vytvoření, efektivního zavedení a udržitelný rozvoj systému řízení bezpečnosti informací. Jedním z organizačních opatření je ustanovení odpovědných osob a jasnou definici jejich odpovědností v systému řízení bezpečnosti informací. Ministerstvo zdravotnictví České republiky je správcem kritické informační infrastruktury, tak jak je definována v ZKB, potažmo ve směrnicí rady 2008/114/ES, ze dne 8. prosince 2008, o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu. Jako správce KII má mimo jiné ministerstvo zdravotnictví České republiky za povinnost identifikovat organizační jednotky, kterých se systém řízení bezpečnosti informací týká.

V rámci zvyšování ochrany KII v ČR byla novelizována vyhláška č.437/2017 Sb. o kritériích pro určení provozovatele základní služby s účinností od 1.1. 2021. Tento návrh nepřináší změnu podstaty právní úpravy, ale pouze změnu určujících kritérií v odvětví zdravotnictví tak, aby došlo k přiměřenému rozšíření povinných osob dle zákona o kybernetické bezpečnosti v tomto odvětví. Prostřednictvím navrhované změny by pak mělo dojít k zajištění vyšší míry kybernetické bezpečnosti v odvětví zdravotnictví, které je v současné době vystaveno významnějšímu množství kybernetických bezpečnostních hrozeb a zároveň je nezbytné pro zvládání krizové situace v souvislosti s probíhající pandemií.

Navrhovaná úprava reflektuje vývoj v oblasti kybernetických bezpečnostních hrozeb a jejich cílů, kterými poskytovatelé zdravotních služeb zejména v době pandemie nemoci Covid-19 jsou, a s tím související poznatky aplikační praxe, tedy že počátečně určený okruh poskytovatelů zdravotních služeb se počíná jevit nedostatečným. Na výše popsaný vývoj v této oblasti reagoval i předseda vlády požadavkem vůči ministrovi zdravotnictví sděleným mu dopisem ze dne 31. července 2020, č. j. 26735/2020-UVCR. Tímto dopisem mimo jiné žádal ministra i o spolupráci s NÚKIB na vydefinování kritérií, která by v aplikační praxi byla schopná zahrnout mezi provozovatele základních služeb poskytovatele zdravotních služeb se zohledněním následujících faktorů:

- Regionální rozložení (oblastní rozložení po celém území státu)
- Spádovost
- Unikátnost či významná specifičnost poskytovaných zdravotních služeb
- Možnost efektivní zastupitelnosti dalších zdravotních zařízení (kapacitní hledisko)
- Návaznost na integrovaný záchranný systém (zejména na zdravotnickou záchrannou službu).

Plnění těchto povinností s sebou nese častou nutnost vynaložení finančních prostředků, a to v oblasti pořízení a provozu bezpečnostních opatření, které jsou určení provozovatelé základních služeb povinni zavádět, a zajištění personálních kapacit, pokud k pokrytí rolí sloužících k zajištění kybernetické bezpečnosti nedostačuje současný personál příslušných oddělení.

Tyto náklady poskytovatelů zdravotních služeb se mohou promítnout do více typů rozpočtů. Dle provedených analýz budou nově mezi subjekty povinné ze zákona o kybernetické bezpečnosti zařazeny jak soukromí poskytovatelé zdravotních služeb, tak příspěvkové organizace obcí či krajů či akciové společnosti obcemi a kraji majoritně vlastněné stejně jako subjekty přímo podřízené ministerstvům.

Každý subjekt tak sám vyhodnotí, jaká rizika jsou spojená s provozem jeho informačních systémů. Následně vyhodnocuje vhodná opatření, která VKB nabízí a jejich implementaci může v případě objektivních překážek bránících okamžité realizaci rozložit do delších časových úseků prostřednictvím plánu zvládání rizik. Mimo tento fakt, je nesporné, že každý poskytovatel zdravotních

služeb disponuje jinými druhy poskytovaných služeb, jinou architekturou informačních systémů, které jím poskytované služby podporují, a jinou úrovní již přijatých opatření pro eliminaci kybernetických rizik. Nutné náklady se mohou u jednotlivých poskytovatelů zdravotních služeb významně odlišovat. Tyto náklady rovněž nemohou být poskytovatelům zdravotních služeb předem známy bez provedené analýzy rizik a následných kroků. Jejich vyčíslení, aby bylo způsobilé alespoň rámcově odpovídat realitě, by tak nutně muselo předcházet provedení analýzy rizik, a tedy splnění povinnosti dané zákonem o kybernetické bezpečnosti potažmo VKB ještě předtím, než je daný subjekt vůbec shledán za povinný podle zákona o kybernetické bezpečnosti, a tedy než musí splnit požadavky jeho prováděcí vyhlášky – VKB.

Lze však říci, že dojde k navýšení počtu těchto provozovatelů základních služeb s největší pravděpodobností o přibližně 19 nových subjektů. Jejich počet závisí na naplnění dopadových kritérií a posouzení této skutečnosti ve správním řízení zahájeném až po účinnosti novelizované vyhlášky č.437/2017 Sb. o kritériích pro určení provozovatele základní služby.

Mezi organizace poskytující zdravotní péči jako základní službu je potřeba zařadit a jako nedílnou součást systému poskytování zdravotní péče vnímat organizace, které kapacitou minimálně 400 akutních lůžek spadají do kritéria dle vyhlášky č.437/2017 Sb. o kritériích pro určení provozovatele základní služby, kde jsou uvedena kritéria v příloze, bod 5 v oblasti zdravotnictví a to takto:

<table>
<tr><th colspan="3">Odvětvová kritéria</th><th rowspan="2">Dopadová kritéria</th></tr>
<tr><th>Druh služby</th><th>Druh subjektu</th><th>Speciální kritéria druhu subjektu</th></tr>
<tr><td rowspan="2">5.1. Poskytování zdravotních služeb</td><td rowspan="2">Poskytovatel zdravotních služeb podle zákona o zdravotních službách</td><td rowspan="2">a) Celkový počet akutních lůžek v posledních třech kalendářních letech nejméně 400,</td><td>Dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je závislé poskytování služby, může způsobit</td></tr>
<tr><td>I. závažné omezení druhu služby postihující více než 50000 osob,</td></tr>
</table>

		b) statut centra vysoce specializované traumatologické, onkologické, cerebrovaskulární, kardiovaskulární, komplexní kardiovaskulární nebo perinatologické péče podle zákona o zdravotních službách,	II. závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury,
		c) zajišťování urgentního příjmu podle zákona o zdravotnické záchranné službě v zařízení s celkovým počtem lůžek intenzivní péče v posledních třech kalendářních letech nejméně 40 nebo	III. nedostupnost druhu služby pro více než 1600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů,
		d) poskytovatel akutní lůžkové péče s průměrným počtem unikátních ošetřených pacientů v posledních třech kalendářních letech nejméně 100000 zajeden kalendářní rok.	IV. oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1000 zraněných osob vyžadujících lékařské ošetření,
			V. narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by

			mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému, nebo
			VI. kompromitaci citlivých osobních údajů o více než 200000 osobách.

3.2 SWOT Analýza

SWOT analýza se používá na zhodnocení vnitřních a vnějších faktorů ovlivňujících úspěšnost organizace nebo nějakého konkrétního záměru. Konkrétně se hodnotí silné a slabé stránky, příležitosti a hrozby.

Silné a slabé stránky jsou hodnoceny optikou vlivu vnitřního prostředí organizace a příležitosti a hrozby jsou zase hodnoceny jako důsledky působení vnějších vlivů. SWOT analýza Je také širší součástí řízení rizik, neboť postihuje klíčové zdroje rizik (hrozby), pomáhá si je uvědomit a případně nastavit protiopatření.

Pro vnější faktory platí, že je zapotřebí předem jasně stanovit, co se za ně, s ohledem na analyzovaný problém nebo subjekt, považuje. Vnější faktory jsou pro kontext tohoto dokumentu považovány zejména legislativní požadavky a doporučení autorit jak ve vnitrostátním, tak mezinárodním měřítku. V našem případě je potřeba identifikovat tyto 4 oblasti pro záměr Strategie kybernetické bezpečnosti Ministerstva zdravotnictví České republiky pro období 2021–2025.

Detailní SWOT analýza je součástí odkazů tohoto dokumentu.

Manažerské shrnutí SWOT analýzy prostředí

Silnými stránkami v rámci zavádění kybernetické bezpečnosti sektoru zdravotnictví jsou bezesporu již provedené kroky na centrální úrovni, jasná strategická vize a uvědomění si významu kybernetické bezpečnosti, ale i informatizace a digitalizace resortu obecně, znalost vlastního organizačního i technického prostředí resortu, společně s uvědoměním si nutnosti zavedení kybernetické bezpečnosti. Je vyžadováno metodické vedení ze strany ministerstva zdravotnictví.

Slabinami se pak jeví zejména nedostatečně koordinovaný způsob zavádění kybernetické bezpečnosti, vyplývající z roztříštěnosti organizací resortu z pohledu jejich zřizovatele a modelu řízení a nedostatečných nástrojů pro centrální koordinaci na straně ministerstva, nedostatek odborného personálu v rámci kybernetické bezpečnosti a aktuálně i nenaplňování povinností

poskytovatelů základní služby dle požadavků ZKB a VKB. Kritickou slabou stránkou je pak dlouhodobé podfinancování nejen kybernetické bezpečnosti, ale informačních a komunikačních technologií obecně, a to napříč celým resortem zdravotnictví a všemi jeho oblastmi, a s ním související nahlížení na problematiku digitalizace a informatizace resortu a jeho organizací jako na servisní problematiku, nikoliv jako na klíčový strategický problém, který bude do budoucna dále nabývat na významu a ovlivňovat všechny ostatní aspekty poskytování zdravotních služeb.

Zranitelnosti jsou identifikovány v rámci nepřipravenosti na aplikování nových technologií ve zdravotnictví bez důrazného dodržování požadavků na kybernetickou bezpečnost. Další zranitelností je nedostatek odpovědnosti za zavedení, provozování a rozvoj kybernetické bezpečnosti v řízených organizacích ze strany jejich vedení a tím nedostatečnou alokaci prostředků na prosazování kybernetické bezpečnosti v organizacích. Jedná se o další zranitelností, která přímo ovlivňuje aktuální stav kybernetické bezpečnosti v resortu MZČR.

Příležitosti můžeme nacházet v možnostech čerpat prostředky z fondů EU, pro zajištění zdrojů potřebných pro odpovídající úroveň KB v resortu MZČR. Vytvořením Centra kybernetické bezpečnosti by se vytvořila kompetenční základna pro poskytování metodické podpory kybernetické bezpečnosti. Optimální řešení je synchronizace aktivit z centrální úrovně prostřednictvím Národního centra pro elektronické zdravotnictví a kompetenčních center kybernetické bezpečnosti. Tyto platformy by zastřešovaly aktuální i budoucí výzvy kybernetické bezpečnosti spojené s elektronizací zdravotnictví České republiky. Možným poskytovatelem služby zabezpečené komunikační infrastruktury pro resort MZČR by mohl být jeden ze stávajících poskytovatelů této služby, což poskytuje příležitost sjednotit úroveň zabezpečení komunikační infrastruktury v resortu MZČR a čerpat aktuální zkušenosti poskytovatele v rámci prostředí poskytovatelů zdravotní péče v České republice.

3.3 Analýza stakeholderů

Detailní analýza stakeholderů v kontextu tohoto dokumentu je uvedena v příloze č. 3. Při rozdělení stakeholderů do jednotlivých skupin byla brána zejména významnost jednotlivých typů organizací a dopad, který mají na systém poskytování zdravotní péče v České republice.

Dopadová kritéria pro určení kritičnosti organizace vzhledem k nutnosti zajištění kybernetické bezpečnosti jsou tyto:

1. **Nízký dopad** (organizace kontrolované a metodicky vedené MZČR s požadavkem na zajištění minimální stanovené úrovně organizačních a technických opatření v rámci kybernetické bezpečnosti),
2. **Střední dopad** (organizace kontrolované NÚKIB a metodicky vedené MZČR, povinné řídit se ZKB. Požadavek na zajištění optimální úrovně organizačních a technických opatření),
3. **Vysoký dopad** (organizace kontrolované NÚKIB, povinné řídit se ZKB. Narušení provozuschopnosti těchto zařízení může mít významný dopad na schopnost zajistit zdravotnické služby v rámci systému poskytování zdravotní péče).

Manažerské shrnutí SWOT analýzy stakeholderů

Organizace s vysokým dopadem:

Mezi tyto organizace primárně patří MZČR, ÚZIS, SÚKL, KHS, správci a provozovatelé KII/VIS.

Silnými stránkami těchto organizací jsou znalosti vlastního prostředí, již identifikované potřeby pro efektivní řízení KB a v neposlední řadě také dostatek prostředků k implementaci opatření pro podporu KB, jak na organizační, tak technické úrovni.

Slabými stránkami jsou pak chybějící koordinovaný způsob zavádění kybernetické bezpečnosti, spolu s nejednotným přístupem ke KB, který nedává záruku efektivní ochrany klíčových dat, a informací a správného nastavení procesů.

Příležitosti jsou identifikovány jako možnosti využít metodické podpory ze strany centrálních organizací NÚKIB a Ministerstva zdravotnictví ČR. Klíčovou příležitostí je možnost využití zdrojů v rámci Evropských strukturálních fondů, v rámci Národního plánu obnovy a integrovaného regionálního operačního programu.

Nejvýznamnější hrozbou se jeví nedostupnost služeb v důsledku kybernetického bezpečnostního incidentu. Hrozbou je i přetrvávající přehlížení hrozeb KB, nedostatečné nastavení odpovědnosti managementu a nedostatečná míra povědomí o kybernetické bezpečnosti na všech úrovních.

Organizace se středním dopadem:

Mezi tyto organizace primárně patří provozovatelé základní služby, zdravotnická zařízení veřejné správy a samosprávy, zdravotní pojišťovny.

Silnými stránkami těchto organizací je opět znalost vlastního ICT prostředí s návazností na snadnější identifikaci oblastí ke zlepšení a omezený objem zpracovávaných zejména zdravotních informací.

Slabými stránkami jsou: nedostupnost metodické podpory a vedení v rámci resortu MZČR, chybějící sdílené služby, které by mohly organizace využívat, chybějící a nedostupní odborníci na oblast KB, nedostatečné povědomí a odpovědnost vedení organizací v souvislosti s KB.

Příležitostí je možnost využití zdrojů v rámci Evropských strukturálních fondů. Dále možnost využití metodické podpory ze strany MZČR a NÚKIB. Do budoucna pak využití sdílení znalostí v rámci resortu, stejně tak jako využití sdílení nákladných technologických řešení pro zajištění KB v rámci resortu MZČR.

Nejvýznamnější hrozbou se jeví nedostupnost služeb v důsledku kybernetického bezpečnostního incidentu. Hrozby pro tyto organizace jsou pak identifikovány z nedostatečné míry povědomí o kybernetické bezpečnosti na všech úrovních a nedostatečné pokrytí technologickými a organizačními opatřeními, způsobenými jejich náročností na realizaci, pořízení a zabezpečení udržitelného provoz.

Organizace s nízkým dopadem:

Mezi tyto organizace primárné patří malá zdravotnická zařízení soukromé sféry, ambulantní zdravotnická zařízení, poskytovatelé zdravotnického materiálu.

Silnými stránkami je možnost snadného ošetření KB prostředky ochrany pracovních stanic, nebo relativně jednoduchého řešení v rámci malého zdravotnického zařízení disponujícího pouze omezeným počtem výpočetní technicky a zdravotnických prostředků. Silnou stránku je rovněž integrované řešení KB ze strany renomovaných dodavatelů IT technologií.

Slabými stránkami jsou nedostatek sdílených informací mezi organizacemi, chybějící závazná legislativní povinnost pro zavedení, údržbu a rozvoj KB v organizaci se zodpovědností vedení organizace, stejně tak jako absence definovaných minimálních organizačních a technických opatření pro zajištění KB.

Příležitosti jsou identifikovány v oblastech možnosti metodické podpory ze strany MZ a kompetenčních center KB, které nastaví pravidla a minimální požadavky na KB těchto organizací, kterými se budou řídit dodavatelé IT řešení. V neposlední řadě také využití sdílených služeb/prostředků ekonomicky náročných na zavedení a provoz, v rámci resortu zdravotnictví.

Hrozbami byly identifikovány neznalosti odborného personálu o aktuálních hrozbách a zranitelností, vyplývajících z nízké úrovně bezpečnostního povědomí a navazující neschopnost efektivně chránit klíčové informace a procesy.

3.4 Obsahové domény

Celá strategie byla na základě provedených analýz rozdělena na několik obsahových domén, kterým odpovídají i formulované globální cíle popsané v kapitole 5 Soustava cílů. Jedná se o následující obsahové domény:

Řízení informační bezpečnosti

a. Technické aspekty kybernetické bezpečnosti
b. Zvyšování bezpečnostního povědomí
c. Kybernetická bezpečnost elektronického zdravotnictví
d. Kybernetická bezpečnost zdravotnických prostředků

4 Vize kybernetické bezpečnosti resortu zdravotnictví

Kybernetická bezpečnost je nedílnou součástí poskytování moderních zdravotních služeb, Oblast kybernetické a informační bezpečnosti bude systematicky rozvíjena a podporována tak, aby byla zajištěna dostupnost a bezpečnost poskytování zdravotních služeb.

V oblasti zdravotnictví jsou rozvíjeny a široce uplatňovány standardy a procesy zaměřené na zvyšování kybernetické a informační bezpečnosti.

5 Soustava cílů

V souladu se závěry provedených analýz a formulovanými hlavními obsahovými doménami (viz kapitolu 3.4 Obsahové domény) bylo definováno pět globálních strategických cílů, které jsou následně v rámci níže popsané soustavy rozpracovány na jednotlivé strategické cíle a na specifické cíle které představují základní realizační jednotku Strategie kybernetické bezpečnosti. Pro každý strategický cíl jsou definováni klíčoví aktéři, termíny realizace a předpokládané zdroje využité pro jejich realizaci. Rozpracování cílů v odpovídajícím detailu bude realizováno formou pracovních skupin, které rozpracují globální cíle do odpovídajících strategických cílů za účelem vytvoření odpovídajícího akčního plánu k naplnění těchto strategických cílů.

GC1 Zavedení řízení bezpečnosti informací jako mandatorního procesu všech poskytovatelů zdravotních služeb

Cílem je formulace zásad pro zavedení systému řízení bezpečnosti informací jako mandatorní součástí systému řízení všech poskytovatelů zdravotních služeb. V návaznosti na formulaci zásad je hlavním cílem zavedení systému řízení bezpečnosti informací do praxe, které bude realizováno prostřednictvím legislativního návrhu zakotvujícího zásady pro uplatnění odpovědnosti managementu organizace za kybernetickou bezpečnost.

GC2 Zajištění minimálního technického standardu kybernetické bezpečnosti

Vytvoření minimálního technického standardu a pomocí definovaných technických opatření a řešení, dosáhneme nastavení společně definované minimální akceptovatelné úrovně zajištění kybernetické bezpečnosti u poskytovatelů zdravotních služeb. Pro naplnění cíle je klíčové vypsání finančních programů zaměřených na rozvoj kybernetické bezpečnosti ve zdravotnictví včetně stanovení rozsahu nároků na financování pro jednotlivé typy subjektů.

GC3 Zvyšování bezpečnostního povědomí

Bezpečnostní povědomí a jeho budování je nedílnou součástí konceptu udržitelné a rozvoje schopné kybernetické bezpečnosti. Plánovaně bude bezpečnostní povědomí rozšiřováno u širokých vrstev uživatelů, zdravotnického personálu a veřejnosti.

GC4 Vytvoření kompetenčního centra KB

Cílem je vytvoření kompetenčního Centra kybernetické bezpečnosti (CKB) a jeho začlenění jako organizační součásti NCEZ jako organizační součásti resortu Ministerstva zdravotnictví. Součástí cíle je příprava a schválení koncepce sdílených technických, metodických a konzultačních služeb CKB v návaznosti na detailní zmapování potřeb organizací resortu a navázání koordinace a spolupráce s klíčovými aktéry v oblasti KB.

GC5 Kybernetická bezpečnost zdravotnických prostředků

Cílem je definice typů zdravotnických prostředků, u kterých je žádoucí provádět a publikovat hodnocení kybernetické bezpečnosti. Dále je součástí cíle vytvoření definice formálního rámce pro posouzení (a veřejnou publikaci) míry kybernetické bezpečnosti zdravotnických prostředků. Součástí cíle je navázání spolupráce s orgány zajišťujícími certifikaci zdravotnických prostředků a nalezení formálního základu pro tvorbu katalogu, které se promítne do podpisu memoranda o spolupráci s atestačními středisky zdravotnických prostředků.

6 Přílohy:

Součástí strategie jsou následující přílohy uvedené v samostatném dokumentu:

Příloha č. 1	SWOT Analýza současného stavu
Příloha č. 2	PESTL Analýza současného stavu
Příloha č. 3	Analýza stakeholderů