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 - přílohy

Pořadí revize	Provedené dne	Zpracoval	Schválil
1.0	1.7. 2021	Tomáš Bezouška manažer kybernetické bezpečnosti	Martin Zeman předseda výboru pro řízení kybernetické bezpečnosti

Obsah

Seznam obrázků

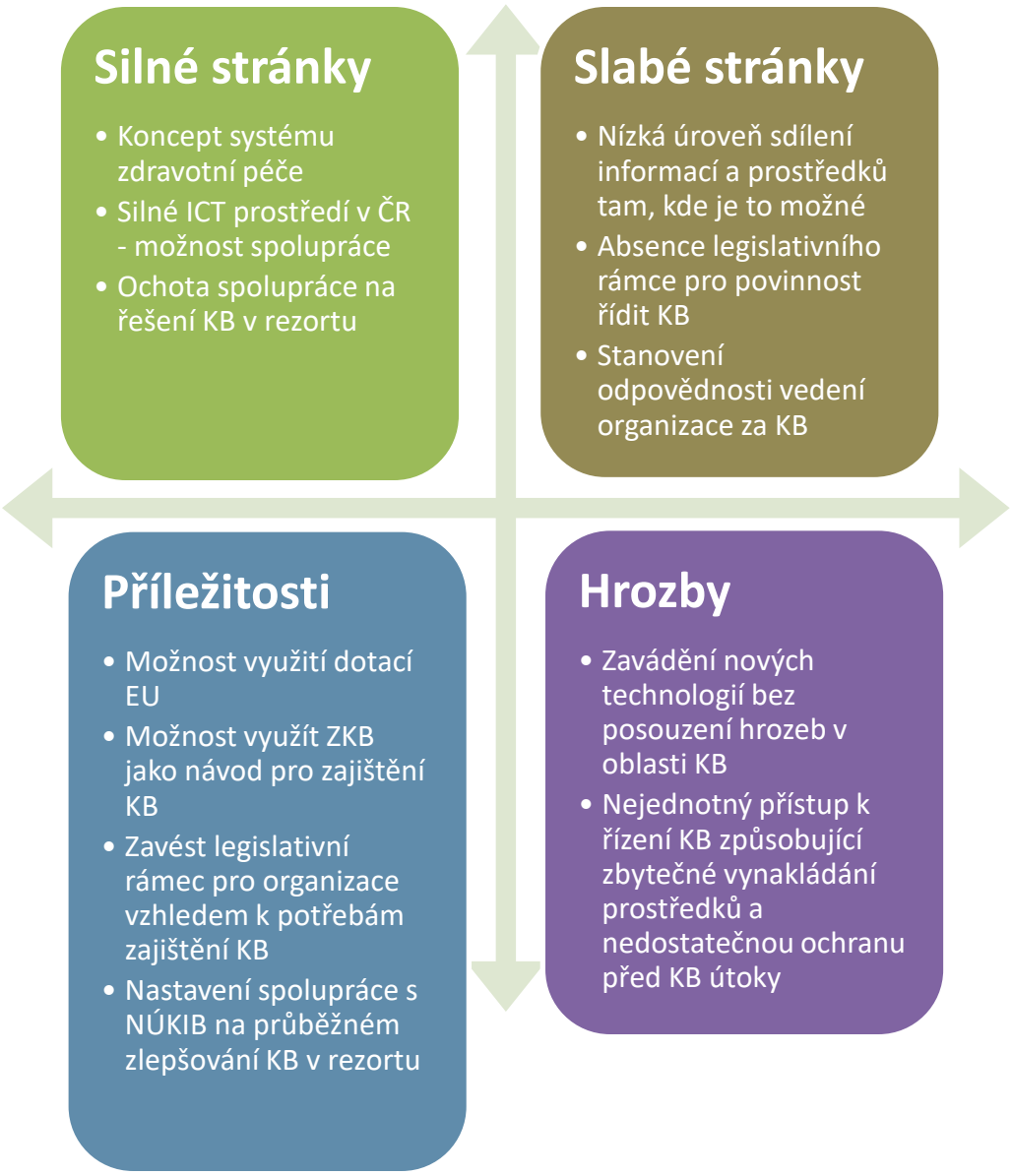
Seznam zkratek a pojmů

Zkratka	Význam
ICT (IKT)	Informační a komunikační technologie (Information and Communication Technology)
ITEZ (CKB NCEZ)	Odbor ITEZ, centrum kybernetické bezpečnosti Národního centra elektronického zdravotnictví
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
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

Přílohy Strategie kybernetické bezpečnosti resortu zdravotnictví České republiky

1.1 Příloha č. 1 SWOT analýza současného stavu



Obrázek 1 SWOT analýza současného stavu

Silné stránky

Silné stránky jsou interní a pozitivní faktory, které pomohou využít příležitostí ve vnějším prostředí.

Mezi silné stránky v kontextu tohoto dokumentu bezesporu patří samotný systém zdravotní péče, který díky své koncepci se vyznačuje přirozenou odolností, vycházející z toho, že Česká republika má kvalitní síť zařízení poskytujících zdravotní péči, a tak výpadek jednotek těchto zařízení z pohledu celku nijak zásadně neovlivňuje schopnost systému poskytování zdravotní péče jako takového, plnit svou funkci.

Také záměr a strategie resortu Ministerstva zdravotnictví České republiky, jako jasný krok vedoucí k rozvoji systému řízení bezpečnosti informací, je výhodou a silnou stránkou demonstrující záměr řídit bezpečnost zdravotnických informací nejen na straně Ministerstva zdravotnictví České republiky. Tento záměr, tedy řídit jednotně kybernetickou bezpečnost, se vztahuje na celé prostředí zdravotnictví a dává si za cíl strategicky řídit kybernetickou bezpečnost jako klíčovou složku rozvoje elektronického zdravotnictví. Dalším krokem musí být prosazení sytému řízení bezpečnosti informací do celého resortu Ministerstva zdravotnictví České republiky. Jedině tento krok může zajistit ucelenou a efektivní ochranu nejen informací a dat v rámci samotného Ministerstva zdravotnictví České republiky, ale zejména u dalších organizací poskytujících zdravotní péči, nehledě na jejich velikost a úroveň zavedených procesů systému řízení bezpečnosti informací. Přirozeným krokem s cílem nastavit jasná pravidla v oblasti kybernetické bezpečnosti resortu MZČR je i tvorba architektury prostředí resortu, jako nedílného kroku v rámci plánování budoucího řízení kybernetické bezpečnosti. Tento architektonický model, bude po diskusi s odpovídajícími autoritami na úrovni Odboru hlavního architekta ministerstva vnitra České republiky zajišťovat jeho udržitelnost a další rozvoj v souladu se záměry eGovernmentu ČR.

Prostředí České republiky také poskytuje širokou škálu spolupráce mezi oblasti zdravotnictví a lokálním ICT prostředím, odborníky a firmami. V tomto prostředí zaujímají významnou pozici také společnosti zabývající se výzkumem a vývojem technologií a postupů na poli kybernetické bezpečnosti. Vyskytuje se zde tedy široké zastoupení odborníků, kteří aktivně přispívají k boji pro kybernetické kriminalitě. Tento fakt se promítá do možnosti spolupracovat při vývoji bezpečnostních řešení na míru, nebo pro specifické potřeby oblasti zdravotnictví.

Slabé stránky

Mezi slabé stránky zdravotnictví, v rámci kontextu tohoto dokumentu, aktuálně mimo jiné patří neexistence zásad pro uplatnění odpovědnosti managementu jednotlivých institucí zapojených do poskytování zdravotní péče v České republice. Tento dokument nade vše pochybnosti stanovuje jasnou a nepopiratelnou odpovědnost managementu dané instituce za ochranu informačních aktiv v organizaci. Zejména otázka zajištění zdrojů a jmenování osob pro implementaci efektivního a udržitelného systému řízení informační bezpečnosti. Management se také musí aktivně a pravidelně zajímat o situaci v oblasti kybernetické bezpečnosti.

Dalším slabým místem je nízká úroveň sdílení informací, které mohou napomoci včas reagovat a snižovat rizika specifická pro oblast zdravotnictví. Zvyšování bezpečnostního povědomí společně s nedostatečnou kvalifikací, je tak stále slabou

stránkou na všech úrovních a týká se jak uživatelů, přes ICT pracovníky, odborné pracovníky, vedení až k samotným útvarům zabývající se kybernetickou bezpečností.

Nedostatek zdrojů, zejména finančních, znemožňuje zavedení opatření pro zajištění kybernetické bezpečnosti nejen na organizační úrovni (např. zaměstnání odborníků KB), ale také zavedení technických opatření (nákup a provoz technologií zajišťujících KB).

Dalším slabým místem je bezesporu chybějící systém řízení bezpečnosti informací jako rozsah aspoň minimálních požadavků pro zajištění kybernetické bezpečnosti. Tento systém řízení bezpečnosti informací se skládá z mimo jiné z minimálních organizačních a technických opatření pro zajištění bezpečnosti chráněných aktiv.

Dalším faktorem se také jeví aplikační a softwarová různorodost ICT prostředí, která komplikuje nasazení technologických prostředků pro zajištění KB.

Motivace personálu hraje roli zejména v prevenci chyb a ochoty učit se novým věcem, což je zejména v dnešní době neoddělitelná součást každodenních povinností pracovníka na jakékoliv úrovni, zajišťujícího provoz ICT prostředí.

K pokrytí slabých stránek resortu Ministerstva zdravotnictví České republiky je potřeba zejména stanovení přímé zodpovědnosti managementu jednotlivých organizací za implementaci, efektivní udržování a rozvoj kybernetické bezpečnosti. Mezi povinnosti managementu musí být zařazena povinnost nejen zajišťovat zdroje, ale také se aktivně podílet na rozvoji a správě systému řízení bezpečnosti informací.

Bude také potřeba, jako další krok pro zajištění pokrytí slabých stránek resortu MZČR, stanovit minimální požadavky na kybernetickou bezpečnost, a to jak v oblasti organizačních opatření, tak v oblasti technických opatření. Organizační opatření budou primárně pokrývat obsazení bezpečnostních rolí spojených s udržováním kybernetické bezpečnosti, stanovením jejich práv a povinností. Zavedení Centra kybernetické bezpečnosti a Národního centra elektronického zdravotnictví významně přispěje ke stanovení kompetenčních center s potřebnými zdroji pro zajištění odpovídajících služeb v oblastech kybernetické bezpečnosti a elektronického zdravotnictví. U technických opatření pak minimální nutné požadavky pro zajištění odpovídajícího stupně ochrany informačních aktiv organizace resortu MZČR.

Příležitosti

Příležitost je v managementu rizik pojem, který označuje pozitivní podnikatelské riziko. Jedná se např. o vývoj nového produktu, možnost získat podíl na trhu po zkrachovalé konkurenci. Na příležitosti jako typ rizika se často zapomíná, přestože mohou mít na budoucí stav organizace velký vliv. Je tedy vhodné příležitosti využívat a nedovolit, aby se změnily na negativní rizika.

V rámci identifikovaných příležitostí se oblast zdravotnictví České republiky musí připravit na rostoucí snahu používání nových technologií a dalších prvků zpracovávajících zdravotnické informace. V tomto směru je možnost nastavení spolupráce s komerčním sektorem KB, který je v prostředí České republiky velmi silný. Další spoluprací mohou být vysoké školy a jejich možnosti výzkumu.

Řídit bezpečnost informací jak na úrovni Ministerstva zdravotnictví České republiky, tak na úrovni resortu, nelze bez zajištění potřebných zdrojů v souladu s požadavky ZKB a VKB, kde se uvádí v §3 bod j)“ řídí provoz a zdroje systému řízení bezpečnosti informací a zaznamenává činnosti spojené se systémem řízení bezpečnosti informací a řízením rizik“. S ohledem na provedené zmapování potřeb poskytovatelů zdravotních služeb v oblasti kybernetické bezpečnosti je nezbytné zajištění financování v této oblasti v řádu vyšších jednotek miliard Kč, bez kterého se nepodaří eliminovat současný technologický dluh jednotlivých organizací v této oblasti. Společně s tvorbou strategie pro roky 2021-2025, probíhají kroky související se zajištěním a efektivní distribucí finančních zdrojů na rozvoj kybernetické bezpečnosti v resortu zdravotnictví. Zejména se jedná o finanční zdroje z Evropských fondů v programovém období 2021-2027. Zajištění zdrojů, a nejen finančních je nedílnou součástí úspěšného naplnění strategie realizováním jejich cílů

Pro zavedení jednotného systému řízení bezpečnosti informací je zde možnost využít ZKB. Pro některé organizace v rámci zdravotnictví je to povinnost, jako pro poskytovatele základní služby, nebo jako správce KII/VIS, pro ostatní organizace to může být příležitost, jak zavést systém řízení bezpečnosti informací do jejich prostředí.

V souladu s požadavky programu Digitální Česko, zejména pak Digitální ekonomika a společnost je potřeba vnímat, že Česká republika se aktivně zapojuje do výzkumných a vývojových aktivit v rámci jednotného digitálního trhu. Klíčové je zejména efektivní zaměření týkající se zpracovávání enormního množství (objemu) dat, s cílem jejich efektivního využívání pro aktuální potřeby i budoucí výzvy digitální ekonomiky a služeb. Nové technologie významným způsobem přispívají k řešení klíčových socioekonomických výzev např. v oblasti zdravotnictví (návrh nových léčiv a personalizovaná medicína).

Podpora digitalizace, nových technologií a nových organizačních modelů ve všech výše nevyjmenovaných (ostatních) sektorech lidské činnosti, a to zejména podpora digitálního (elektronického) zdravotnictví v kontextu této Strategie, jsou dalším z kroků podporujících rozvoj programu Digitální Česko.

Rozvojové aktivity pro vzdělávání v oblasti kybernetické bezpečnosti, které jsou reflektovány zejména v potřebách rozvoje vzdělávání v oblasti kybernetické bezpečnosti, která je jednou, nikoliv však jedinou podmínkou pro efektivní a udržitelný rozvoj nejen digitalizace v oblasti zdravotnictví. Do procesu zvyšování bezpečnostního povědomí je potřeba zapojit nejen profesionály na straně resortu Ministerstva zdravotnictví České republiky, ale také prostřednictvím zdravotních pojišťoven zejména veřejnost. Je také potřeba zajistit prostředky a zdroje na tyto vzdělávací projekty, bez kterých se požadovaný výstup nemá šanci realizovat. Soustředěním znalostí, zkušeností a kompetencí do Centra kybernetické bezpečnosti v rámci resortu MZČR, společně s Národním centrem pro elektronické zdravotnictví zajistí možnost poskytování kontinuální metodické podpory při prosazování cílů této Strategie.

Hrozby

Hrozby odkazují na faktory, které mají potenciál poškodit organizaci. Dopady kybernetických útoky se počítají v řádech desítek miliónů, ale mohou být řádově vyšší v případě ochromení velkých nemocnic.

Hrozbou pro zdravotnictví je nárůst kybernetické kriminality se zaměřením zejména na zdravotnické organizace, kde útočníci identifikovali snadnější cíle k dosažení svých záměrů.

Dalším faktorem je mnohdy až živelná snaha digitalizace zdravotních služeb, bez schopnosti správně vyhodnotit a efektivně řídit hrozby v oblasti kybernetické bezpečnosti. Tato hrozba se nevztahuje pouze na zdravotnické organizace, ale také na samotné občany, kteří nejsou schopni správně vyhodnotit rizika v oblasti kybernetické bezpečnosti. Incidenty kybernetické bezpečnosti mají o to větší dopad, čím méně je organizace, nebo prostředí připraveno a testováno na takovouto nenadálou událost.

Hrozbou se tedy naprosto přirozeně jeví nejen chybějící legislativní rámec, který jasně definuje povinnost vedení organizace se aktivně podílet na implementaci a dalším rozvoji systému řízení bezpečnosti informací, včetně zajištění odpovídajících zdrojů, a dále pravidelně tento systém řízení bezpečnosti informací vyhodnocovat a zlepšovat. Aktuálně je takto definovaná povinnost pouze pro osoby povinné podle ZKB, která ovšem pokrývá jen část prostředí resortu Ministerstva zdravotnictví České republiky.

Hrozbou se jeví i nedostatečná inovace v oblasti nejen ICT prostředků ale zejména procesů a systému řízení. Neschopnost reagovat na moderní trendy a požadavky zejména analýzy velkých dat, zpracování a sdílení dat v reálném čase, může do budoucna vytvořit neúměrný tlak na rychlost modernizace, místo plánovaného a pozvolného zavádění inovací a moderních postupů. Je proto nejen nutné sledovat vývoj v oblasti Zdravotnictví 4.0, ale i přizpůsobovat podmínky a technologie, které napomáhají a zejména podporují moderní trendy v oblasti ICT, tak zejména kybernetické bezpečnosti.

1.2 Příloha č. 2 PESTL analýza současného stavu

Zdravotnictví obecně závisí na hodnocení stávajících a blížících se právních předpisů, změn trhu a ekonomiky, společenských změn v čase a technologického pokroku. Politická stabilita je vždy důležitým faktorem, protože změna ve vládách může a ovlivňuje nemalou měrou také sektor zdravotnictví a prostředí České republiky obecně.

Zdravotnictví je nejrychleji rostoucím „průmyslovým“ odvětvím v ekonomickém systému jakékoli země. Toto odvětví je rozděleno do tří kategorií zdravotní činnosti, zubní a lékařské činnosti spolu s různými dalšími praktikami v oblasti lidského zdraví.

PESTL analýza je analytická technika sloužící ke strategické analýze okolního prostředí organizace. PESTL je akronym a jednotlivá písmena znamenají různé typy vnějších faktorů:

- P – Political – politické – existující a potenciální působení politických vlivů
- E – Economical – ekonomické – působení a vliv místní, národní a světové ekonomiky
- S – Social – sociální – průmět sociálních změn dovnitř organizace, součástí jsou i kulturní vlivy (lokální, národní, regionální, světové)
- T – Technological – technologické – dopady stávajících, nových a vyspělých technologií
- L – Legal – legislativní – vlivy národní, evropské a mezinárodní legislativy

Podstatou PESTL analýzy je identifikovat pro každou skupinu faktorů ty nejvýznamnější jevy, události, rizika a vlivy, které ovlivňují nebo budou ovlivňovat organizaci. Metoda PESTL je součástí metod používaných v oblasti analýzy dopadů. Někdy bývá použita jako vstup analýzy vnějšího prostředí do SWOT analýzy.

Politické vlivy

Dopad politického prostředí na výkonnost zdravotnictví se neustále mění, zejména kvůli měnícím se vládním předpisům a nařízením. Mnoho ekonomik po celém světě zavedlo způsoby, jak omezit výdaje ve zdravotnictví.

Politické faktory, jako je změna daňových zákonů, zaměstnaneckých předpisů, zákonů na ochranu spotřebitele a pověření k pojištění, mohou mít dopad na zdravotnický průmysl. Prosazování cílů spojených s politicky motivovanými očekáváními mohou mít výrazný dopad na schopnost prosazování cílů spojených s KB.

Ekonomické vlivy

Úroveň nezaměstnanosti, úrokové sazby, dostupnost úvěrů a inflace jsou ekonomické faktory, které ovlivňují výkonnost a fungování zdravotnictví. Tyto změny ekonomického prostředí mohou výrazně ovlivnit výdajovou politiku společností a nákupní chování spotřebitelů. **Nedostatek zdrojů** a zejména

finanční podpora mohou výrazně omezit až znemožnit prosazování cílů spojených se zavedením kybernetické bezpečnosti nejen v resortu MZČR.

Sociální vlivy

Sociálně kulturní faktory se zaměřují na problémy, jako je preference pohlaví, stárnutí populace, snížená plodnost spolu s vírou, hodnotami a normami, které konkrétní spotřebitelský segment zastává. Je velmi důležité, aby organizace určovaly a ovlivňovali kulturu svých spotřebitelů, aby nedocházelo k porušování hodnot, přesvědčení a zvyků.

Lidé jsou nyní více informováni. V jejich očekávání došlo k velké změně směrem k nabídce, rozsahu služeb a nyní jsou stále náročnější. Zejména oblast elektronických služeb se dramaticky rozšiřuje a tyto služby je potřeba zajistit z hlediska kybernetické bezpečnosti.

Technologické vlivy

Technologické faktory ve skutečnosti poskytují zdravotnickým společnostem vynikající příležitosti k růstu. Vývoj počítačových aplikací může pacientům umožnit rychlejší ošetření nebo péči než dříve kdykoliv dříve. Nyní několik společností poskytujících zdravotní péči nabízí aplikace, které mají lékaři spojit se svými pacienty. Několik zdravotnických institucí navíc umožňuje uskutečnění živého chatu nebo e-mailu lékařům s dotazem na jejich nemoc, a to v reálném čase. Je to přirozená fúze technologického pokroku a poptávky.

S prudkým nárůstem možnosti využití technologií i ve zdravotnictví, automaticky vzrostl požadavek i na zaštítění nových funkcionalit poskytovaných různými prostředky z hlediska bezpečnosti zpracovávaných, přenášených i ukládaných informací

Aktuálně lze využít nejen technologické základny budovaných řešení kybernetické bezpečnosti v rámci resortu Ministerstva zdravotnictví České republiky, ale také je doplnit o další zdroje, jako jsou vědomosti, personál a další, které jsou aktuálně již k ochraně klíčových aktiv používány. Lze tak poskytnout i menším organizacím možnost, využívat vyspělé technologie k možnosti odpovídajícím a efektivním způsobem chránit zdravotnické informace. Zároveň je tato cesta také ekonomicky mnohem výhodnější, protože si každá instituce nebude muset budovat svůj vlastní personál a technologické prostředky pro zajištění adekvátní ochrany zdravotnických informací. Tyto synergické efekty bude možno plně využít až s nasazením legislativy, která minimálně definuje:

- Řízení informační bezpečnosti
  - Odpovědnost managementu
  - Systém řízení bezpečnosti informací
- Technické aspekty kybernetické bezpečnosti
  - Definice minimálního technického standardu
  - Základní technologická úroveň kybernetické ochrany
- Zvyšování bezpečnostního povědomí
  - Standardy vzdělávání v kybernetické bezpečnosti

    - Resortní školící program
- Kybernetická bezpečnost elektronického zdravotnictví
    - Centrální technické a sdílené služby
    - Centrální metodické služby
    - Standardy, atestace a certifikace
- Kybernetická bezpečnost zdravotnických prostředků
    - Bezpečnostní standardy ZP
    - Monitoring hrozeb
    - Katalog zdravotnických prostředků

1.3 Příloha č. 3 analýza stakeholderů

Tato kapitola popisuje jednotlivé subjekty, které jsou zapojeny do systému poskytování zdravotní péče v rámci resortu zdravotnictví a jejich vztah v rámci kontextu tohoto dokumentu. Dle vyjádření Národního úřadu pro komunikační a informační bezpečnost, se v období 2021 a dále budou zaměřovat zejména na kontrolu zajištění kybernetické bezpečnosti u provozovatelů základní služby dle ZKB. Dále pak budou upravovat dopadová kritéria, která jsou určující pro stanovení povinnosti řídit se ZKB.

Snahou je popsat vztah organizace v jednotlivých skupinách k problematice řízení kybernetické bezpečnosti, a to nehledě na to, zda jsou poskytovateli základní služby, správci, nebo provozovateli KII/VIS, či nikoliv. Pohledem k významnosti jednotlivých organizací bude hledisko dopadu v případě kybernetického bezpečnostního incidentu. Znamená to tedy, co se stane (dopad na pacienty a vlastníky zdravotnických informací), když bude organizace zasažena kybernetickým bezpečnostním incidentem. Je potřeba brát v úvahu zejména citlivost zpracovávaných informací, které jsou dle GDPR v kategorii zvláštní osobní údaje. Do kategorie zvláštní osobní údaje patří takové údaje, které mohou subjekt údajů samy o sobě poškodit ve společnosti, v zaměstnání, ve škole či mohou zapříčinit jeho diskriminaci. Dalším kritériem je schopnost organizace zasažené kybernetickým bezpečnostním incidentem nadále poskytovat zdravotnické úkony. Při určování dopadových kritérií bylo přihlédnuto zejména ke dvěma aspektům:

- prvním aspektem je objem a rozsah zpracovávaných zdravotních informací
- druhým aspektem je důležitost organizace vzhledem ke schopnosti resortu zdravotnictví zajistit systém poskytování zdravotní péče.

Organizace úrovně 3 – vysoký dopad

Organizace identifikované jako správci, nebo provozovatelé KII/VIS jsou povinné naplňovat požadavky na KB dle ZKB. Kontrolou naplňování požadavků ZKB, stejně jako metodickou podporou je pověřen NÚKIB. MZČR zajišťuje metodickou podporu, stanovuje požadavky a kontroluje jejich naplňování u všech ostatních organizací v resortu.

Mezi rizika v rámci kontextu tohoto dokumentu, která Ministerstvo zdravotnictví České republiky řídí, se řadí zejména nedostupnost a integrita infrastruktury centrálních registrů, hygienických registrů a dalších resortních informačních systémů.

Pro další rozvoj organizací spravující, nebo provozující KII/VIS v oblasti kybernetické bezpečnosti je potřeba zejména navazovat na již provedené kroky v oblasti kybernetické bezpečnosti a další prohlubování a prosazování jednotného přístupu v rámci resortu MZČR k systému řízení bezpečnosti informací. Poskytování metodického vedení a metodické podpory ze strany MZČR, bude jedním ze strategických cílů pro období 2021–2025. Ministerstvo

již v tuto chvíli má personální a zejména znalostní kapacity, které v ostatních organizacích chybí a jsou nedílnou součástí efektivního a udržitelného systému řízení bezpečnosti informací.

Pro zajištění souladu s požadavky ZKB a jeho prováděcích vyhlášek je potřeba pravidelně vyhodnocovat stav zavedených organizačních a technických opatření. Nedostupnost služeb provozovatelů KII/VIS, způsobená kybernetickým bezpečnostním incidentem může mít vysoký dopad na celý systém poskytování zdravotní péče v České republice.

Prohlubování bezpečnostního povědomí je další nedílnou součástí rozvoje kybernetické bezpečnosti a v návaznosti na stanovení minimální úrovni organizačních a technických opatření také krokem je sjednocení přístupu k zajištění kybernetické bezpečnosti resortu MZČR. Slabinami se pak mohou jevit chybějící uzákoněné povinnosti organizací resortu MZČR, které by jednoznačně definovali minimální organizační a technické opatření vedoucí k zajištění požadované úrovně kybernetické bezpečnosti.

Resortní technologické centrum Ministerstva zdravotnictví České republiky zajišťuje zejména služby v oblasti informačních a komunikačních technologií pro organizace resortu zdravotnictví. Resortní technologické centrum zajišťuje po technické stránce Ústav zdravotnických informací a statistiky ve spolupráci s ministerstvem. Mezi jinými službami zajišťuje zejména provoz a rozvoj infrastruktury centrálních registrů, hygienických registrů a dalších resortních informačních systémů.

Resortní technologické centrum Ministerstva zdravotnictví České republiky zajišťuje zejména služby v oblasti informačních a komunikačních technologií pro organizace resortu zdravotnictví. Resortní technologické centrum zajišťuje po technické stránce Ústav zdravotnických informací a statistiky ve spolupráci s ministerstvem. Mezi jinými službami zajišťuje zejména provoz a rozvoj infrastruktury centrálních registrů, hygienických registrů a dalších resortních informačních systémů.

Pro další rozvoj resortního technologického centra v oblasti kybernetické bezpečnosti je potřeba zejména zachovat návaznost na již provedené kroky v oblasti kybernetické bezpečnosti a další rozvoj ve spolupráci se správcem KII, tedy MZČR.

Posuzování kybernetické bezpečnosti u zdravotnických prostředků je nedílnou součástí systému řízení bezpečnosti informací, která ale aktuálně není nikde strukturovaně řízena. Zdravotnické prostředky jsou průběžně modernizovány a jsou připojovány do prostředí poskytovatelů zdravotní péče bez toho, aniž by byly vyhodnocovány dopady na kybernetickou bezpečnost. Tento postup však není v souladu v požadavky ZKB a jeho prováděcích vyhlášek. Je tedy potřeba vytvořit bezpečnostní standard, který bude definovat způsob posouzení míry kybernetické bezpečnosti zdravotnických prostředků. Tyto prostředky totiž zpracovávají zdravotnické informace a v případě jejich nezabezpečení odpovídajícím způsobem, může dojít nejen k narušení samotných zdravotních

informací, ale také k možnému zavlečení škodlivého kódu do prostředí organizace v rámci resortu MZČR. Vznik katalogu zdravotnických prostředků by významně napomohl k nastavení a udržení požadované úrovně kybernetické bezpečnosti. Úroveň kybernetické bezpečnosti jednotlivých zdravotnických prostředků by posuzoval orgán, který vznikne navázáním spolupráce mezi orgány zajišťujícími certifikaci zdravotnických prostředků a MZČR.

Rozvoj provozovatelů KII/VIS je tedy potřeba zaměřit na zlepšování sytému řízení bezpečnosti informací na základě pravidelného hodnocení efektivnosti zavedených organizačních a technických opatření. Takovýto kontinuální rozvoj může pomoci naplnit například zřízení kompetenčního centra kybernetické bezpečnosti pro oblast zdravotnictví.

Obrázek 2 SWOT analýza organizací 1.úrovně

Organizace úrovně 2 – střední dopad

MZ ve spolupráci s NÚKIB nastavují a metodicky podporují zavedení a řízení politik a standardů KB. Je potřeba zejména identifikovat primární aktiva dle

požadavků ZKB a porovnat jejich významnost s jejich hodnotou na úrovni uživatelů těchto identifikovaných primárních aktiv (služeb). Dále je potřeba nastavit opatření na organizační a technické úrovni, které zajistí ochranu těchto primárních aktiv odpovídajícím způsobem. Znalost vlastního ICT prostředí významně pomůže identifikovat slabiny a příležitosti každé organizace vzhledem k službám poskytovaným dovnitř i vně organizace. Je potřeba dbát na zřetel taky požadavky ZKB a GDPR ve smyslu posouzení potřeby chránit informace odpovídajícím způsobem.

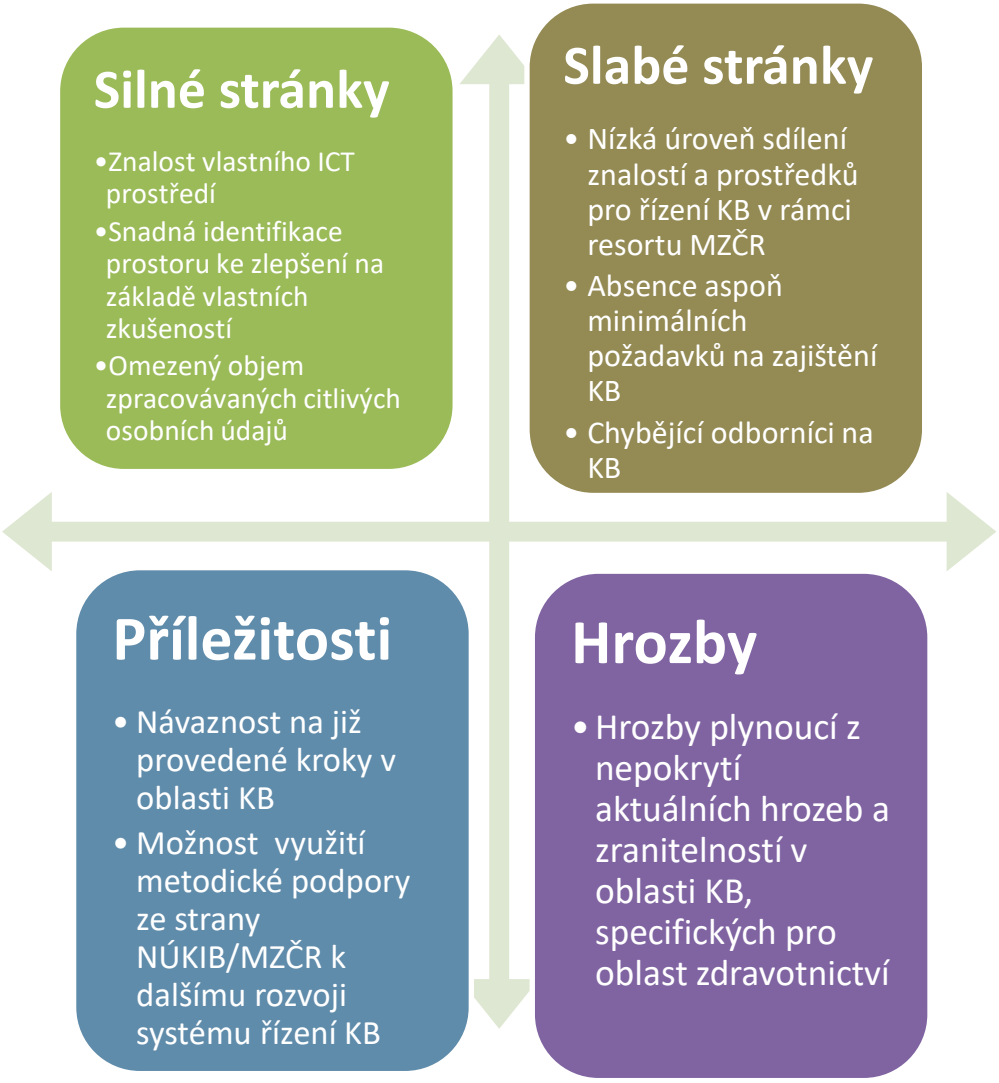
Rizika jsou identifikována zejména v nejednotnosti přístupu k řízení kybernetické bezpečnosti. Existuje tak možnost, že organizace nedostatečně chrání primární aktiva, nebo že je ani není schopna správně identifikovat. Technické zajištění kybernetické bezpečnosti je jedním z dalších rizik, které je potřeba adresovat a neodkladně řešit. Odpovědnost a vztah k povinnosti zajistit kybernetickou bezpečnost stále v mnohých případech není identifikován a neexistuje aktuálně jednotný přístup, jak k organizační požadavkům na kybernetickou bezpečnost přistupovat. Vzdělávání uživatelů na všech úrovních je slabou stránkou, kterou je potřeba začít neodkladně a efektivně řešit. Nejde jen o uživatele samotných informačních systémů, ale také jejich správce. Uživatelé s privilegovanými oprávněními jsou často mimo zájmové skupiny s cílem prohlubování znalostí, a tak jim častokrát chybí informace o aktuálních trendech a zranitelnostech. Mimo uvedené uživatele jsou to i další odborníci v oblasti kybernetické bezpečnosti, kteří aktuálně chybí na všech úrovních organizací.

K rozvoji lze napomoci Centralizovanou správou uvedených aktivit na úroveň MZČR. Je tak možno významně napomoci organizacím k dosažení optimálního stavu řízení informační bezpečnosti. Poskytnutím kontinuálního vzdělávání, metodickou podporou a dalšími kroky lze nejen pomoci, ale zároveň i centralizovaně řídit úroveň kybernetické bezpečnosti v jednotlivých organizacích. Tomu napomůže zřízení kompetenčního centra kybernetické bezpečnosti v rámci resortu, které optimálním způsobem poskytne nejen metodickou podporu, ale také svou publikační činností podpoří snahu ostatních organizací o kontinuální zlepšování systému řízení bezpečnosti informací. Dalším způsobem podpory může být poskytnutí technologické podpory vytvořením centra sdílených služeb kybernetické bezpečnosti, které pomůže organizacím například s monitoringem hrozeb v jejich prostředí, pokud budou do tohoto centra sdílených služeb kybernetické bezpečnosti připojena. Na straně konzumenta těchto služeb tak dojde k významným úsporám času, ekonomických a lidských prostředků.

Organizace by měli posuzovat svůj kontext směrem k ochraně zpracovávaných informací. Pokud jsou tyto informace zdravotnické, podle GDPR by u nich měl být kladen důraz zejména na jejich důvěrnost. Narušení zdravotnických informací důsledkem kybernetického bezpečnostního incidentu s dopadem do integrity a dostupnosti zase skýtá rizika v možnosti poskytovat zdravotní péči. Na základě identifikovaných primárních aktiv je potřeba stanovit optimální

způsob jejich ochrany zejména vzhledem k tomu, jak jsou tato aktiva používána k poskytování zdravotní péče.

K rozvoji bezpečnostního povědomí lze napomoci Centralizovanou správou uvedených aktivit na úroveň MZČR. Tomu napomůže zřízení kompetenční centrum kybernetické bezpečnosti v rámci resortu MZČR, které optimálním způsobem poskytne nejen metodickou podporu, ale také svou publikační činností podpoří snahu ostatních organizací i v soukromé sféře o kontinuální zlepšování systému řízení bezpečnosti informací.



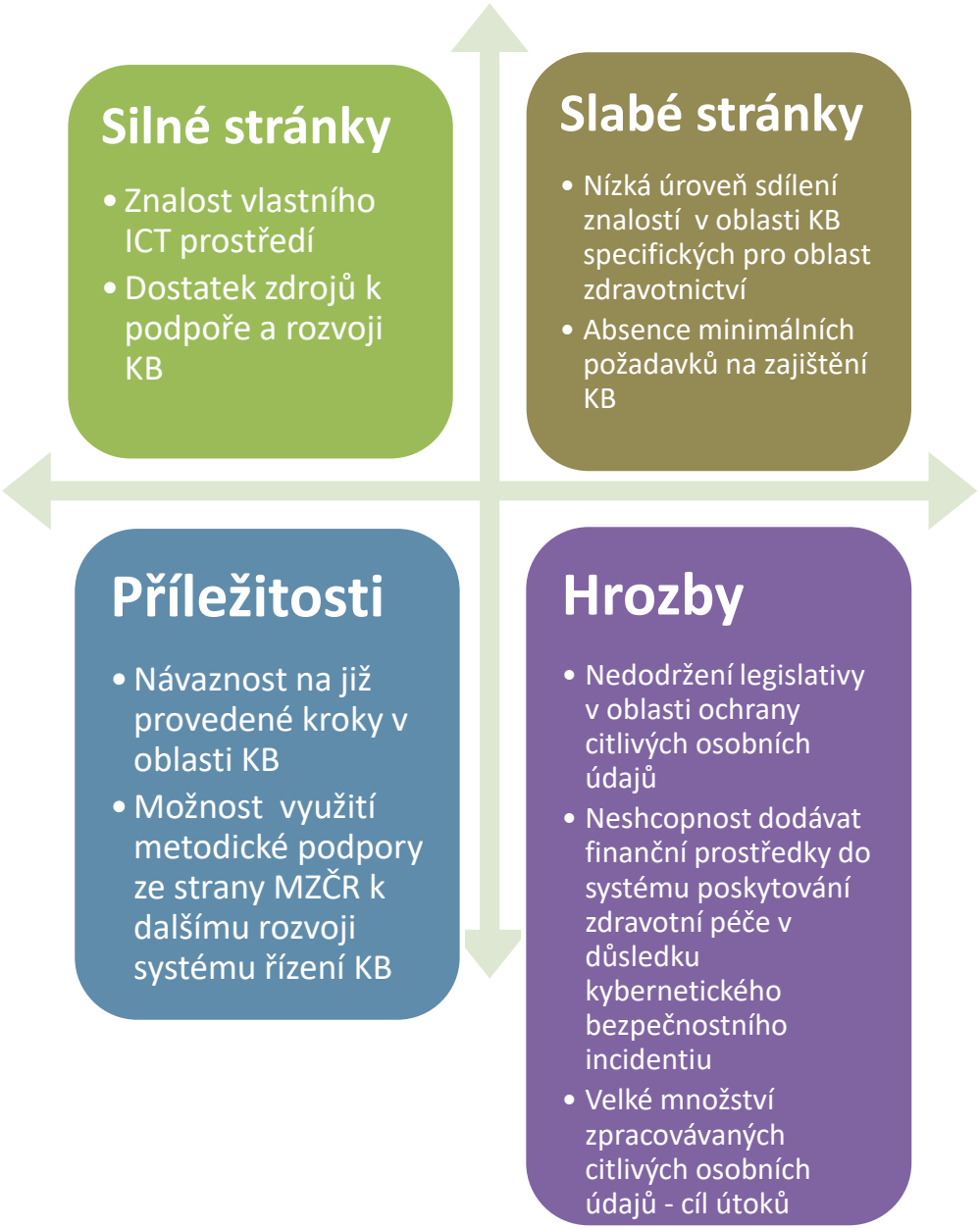
Obrázek 3 SWOT analýza organizací 2.úrovně.

Zdravotní pojišťovny

Zdravotní pojišťovny jsou samostatnou kapitolou mezi organizacemi úrovně 2. Sami o sobě zdravotní pojišťovny neposkytují zdravotní péči, jsou však velmi významným přispěvatelem prostředků na zdravotní péči. Jsou také významnými zpracovateli zdravotnických informací, a proto je potřeba dbát z pohledu zpracovatelů na odpovídající a efektivní ochranu těchto informací.

Rizikovým faktorem je tedy zejména důvěrnost zdravotnických informací, které pojišťovny zpracovávají. Tyto zdravotnické informace jsou také řízeny evropským nařízením pro ochranu osobních údajů GDPR. Zdravotní pojišťovny mají dostatek prostředků pro zajištění odpovídajícího zabezpečení kybernetické bezpečnosti jako na úrovni organizačních opatření, tak z hlediska technických opatření. Zdravotní pojišťovny mají zavedeny i role a odpovědnosti pro zajištění efektivního a udržitelného systému řízení bezpečnosti informací. Z této perspektivy by mělo MZČR zajišťovat jen konzultační a metodickou podporu v rámci kybernetické bezpečnosti.

Ke zlepšení zmapování situace ohledně skutečného stavu kybernetické bezpečnosti je potřeba zavedení standardů pro minimální technické a organizační opatření v rámci kybernetické bezpečnosti resortu MZČR. Následně bude potřeba provést srovnání s těmito požadavky a stanovit nápravná opatření pro případně nalezené neshody.



Obrázek 4 SWOT analýza zdravotních pojišťoven

Organizace úrovně 1 – nízký dopad

Zdravotnická zařízení v úrovni 1 by měla splňovat aspoň minimální požadavky na kybernetickou bezpečnost. MZČR, jako orgán, který metodicky řídí a dohlíží, vydá Standard pro minimální technické a bezpečnostní požadavky pro připojení k centrálním službám. Tento dokument bude mít formu závazného pokynu, který bude určující pro všechny organizace. Vzhledem k velmi omezenému objemu zdravotnických dat a nízký dopad na systém poskytování zdravotní péče, se tyto organizace neřadí ke kritickým organizacím v rámci celého systému poskytování

zdravotní péče. Neznamená to ovšem, že i zde není zapotřebí identifikovat primární aktiva a následně je odpovídajícím způsobem chránit.

Rizikem, kterému zdravotnická zařízení úrovně 1 čelí je nedostatek prostředků na zajištění kybernetické bezpečnosti, stejně jako nedostatek vědomostí na zajištění efektivního rozvoje systému řízení bezpečnosti informací.

K rozvoji zdravotnických zařízení v úrovni 1 přispěje velkou měrou nastavení jednotných standardů pro zajištění kybernetické bezpečnosti. Následně je pak potřeba naplňování těchto standardů pravidelně vyhodnocovat a podnikat kroky k nápravě identifikovaných neshod. Stanovení jasné odpovědnosti za kybernetickou bezpečnost v rámci organizačního zajištění kybernetické bezpečnosti je dalším krokem k naplnění požadavků na řiditelnost s rozvoj systému řízení bezpečnosti informací. Vedle vymahatelnosti odpovědnosti za kybernetickou bezpečnost je potřeba také zajistit prostředky pro její realizaci směrem z vedení jednotlivých organizacích.

Organizace by měli zejména posuzovat svůj kontext směrem k ochraně zpracovávaných informací. Pokud jsou tyto informace zdravotnické, podle GDPR by u nich měl být kladen důraz zejména na jejich důvěrnost. Narušení zdravotnických informací důsledkem kybernetického bezpečnostního incidentu s dopadem do integrity a dostupnosti zase skýtá rizika v možnosti poskytovat zdravotní péči. Na základě identifikovaných primárních aktiv je potřeba stanovit optimální způsob jejich ochrany zejména vzhledem k tomu, jak jsou tato aktiva používána k poskytování zdravotní péče.

Zvyšování bezpečnostního povědomí, je jedním z předpokladů udržitelnosti systému řízení bezpečnosti informací. Je potřeba vzdělávat uživatele na všech úrovních, včetně osob ve vedení organizace.

Lékárny slouží primárně jako distributor zdravotnického materiálu a z pohledu zpracovávaných zdravotnických informací nehrají významnou roli. Stejně tak, jako v rámci systému poskytování zdravotní péče nejsou klíčovým prvkem, který by ohrožoval tento systém. Nicméně i přesto zpracovávají informace, jejichž narušení kybernetickým bezpečnostním incidentem by mohlo mít až fatální následky a to zejména, pokud by došlo k narušení integrity zpracovávaných informací.

Ke zlepšení zmapování situace ohledně skutečného stavu kybernetické bezpečnosti je potřeba zavedení standardů pro minimální technické a organizační opatření v rámci kybernetické bezpečnosti resortu MZČR. Následně bude potřeba provést srovnání s těmito požadavky a stanovit nápravná opatření pro případně nalezené neshody.

Obrázek 5 SWOT analýza organizací 3.úrovně