



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

POSOUZENÍ INFORMAČNÍHO SYSTÉMU FIRMY A NÁVRH ZMĚN

INFORMATION SYSTEM ASSESSMENT AND PROPOSAL OF ICT MODIFICATION

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE

AUTHOR

Adam Sládek

VEDOUCÍ PRÁCE

SUPERVISOR

Ing. Lukáš Novák, Ph.D.

BRNO 2019

Zadání bakalářské práce

Ústav:	Ústav informatiky
Student:	Adam Sládek
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Manažerská informatika
Vedoucí práce:	Ing. Lukáš Novák, Ph.D.
Akademický rok:	2018/19

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává bakalářskou práci s názvem:

Posouzení informačního systému firmy a návrh změn

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současné situace
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem bakalářské práce je popsat a analyzovat současný stav informačního systému VZP a.s. Následně ze zjištěných výsledků analýz vyvodit a navrhnout potřebné změny k jeho lepší funkčnosti a zabezpečení údajů uživatelů.

Základní literární prameny:

BASL, Josef a Roman BLAŽÍČEK. Podnikové informační systémy: podnik v informační společnosti. 3., aktualiz. a dopl. vyd. Praha: Grada, 2012. ISBN 978-80-247-4307-3.

GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi. 3. vyd. Praha: Grada Publishing, 2015. ISBN 978-80-247-5457-4.

SODOMKA, Petr a Hana KLČOVÁ. Informační systémy v podnikové praxi. 2. vyd. Brno: Computer Press, 2010. 504 s. ISBN 978-80-251-2878-7.

TVRDÍKOVÁ, Milena. Aplikace moderních informačních technologií v řízení firmy: nástroje ke zvyšování kvality informačních systémů. Praha: Grada, 2008. ISBN 978-80-247-2728-8.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2018/19

V Brně dne 28.2.2019

L. S.

doc. RNDr. Bedřich Půža, CSc.
ředitel

doc. Ing. et Ing. Stanislav Škapa, Ph.D.
děkan

Abstrakt

Hlavní náplní této bakalářské práce je posouzení informačního systému společnosti VZP, který shromažďuje informace o všech jejích pojištěncích. Přístup k těmto informacím je zprostředkován prostřednictvím firmy Elso Service s.r.o., která pro společnost VZP tento systém spravuje. Práce je rozdělena do teoretické a praktické části. V teoretické části jsou popsány a vysvětleny stěžejní pojmy týkající se problematiky informačních systémů. V praktické části je nejdříve zhodnocen stávající současný stav informačního systému, a to s pomocí určitých analýz s následným návrhem změn, které by měly zlepšit jeho funkčnost.

Klíčová slova

Informační systém, informační bezpečnost, Informace, Data, SWOT analýza, Informační technologie

Abstract

The main idea of this bachelor thesis is to analyse information system of VZP, which contains all information about their clients. Access to this system is provided through company Elso Service s.r.o., which manages it for VZP. There is a teoretical and also practical part. The teoretical part describes and explains the main terms from information system theory. The practical part analyse the present quality of the system and suggests possible solutions for better functionality of the system.

Key words

Information system, Information security, Information, Data, SWOT analysis, Information technology

Bibliografická citace

SLÁDEK, Adam. *Posouzení informačního systému firmy a návrh změn* [online]. Brno, 2019 [cit. 2019-05-07]. Dostupné z: <https://www.vutbr.cz/studenti/zav-prace/detail/119667>. Bakalářská práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Lukáš Novák.

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne __.____ 2019

.....

podpis studenta

OBSAH

ÚVOD.....	10
1 VYMEZENÍ PROBLÉMU A CÍLE PRÁCE.....	11
2 TEORETICKÁ VÝCHODISKA PRÁCE	12
2.1 Data	12
2.2 Informace	12
2.3 Proces	13
2.4 Systém	13
2.5 Hardware	13
2.6 Software	13
2.7 Informační systémy	13
2.7.1 Podnikové systémy	14
2.7.2 Klasifikace podnikových informačních systémů	14
2.8 Relační Databáze.....	19
2.8.1 E-R Diagram (Entitně – Relační model).....	20
2.8.2 Normalizace	20
2.8.3 SQL.....	21
2.9 Informační bezpečnost	21
2.9.1 GDPR.....	22
2.10 Nástroje analýzy	23
2.10.1 SWOT analýza.....	23
2.10.2 Metoda HOS	24
3 ANALÝZA PROBLÉMU A SOUČASNÉ SITUACE	26
3.1 Společnost Elso Service Brno, spol. a.s.	26
3.2 Všeobecná zdravotní pojišťovna.....	27
3.2.1 Konkurence	28

3.3	Infomační systém VZP	30
3.3.1	Uživatelé	33
3.3.2	Hardware a Software	34
3.3.3	Bezpečnost	36
3.3.3.1	Zálohování	37
3.3.4	Práce v systému	37
3.3.5	Správa systému	41
3.4	Analýzy	42
3.4.1	SWOT analýza IS	43
3.4.1.1	Silné stránky	44
3.4.1.2	Slabé stránky	44
3.4.1.3	Příležitosti	45
3.4.1.4	Hrozby	45
3.4.2	HOS analýza IS	46
3.4.2.1	Zjištěné nedostatky	48
3.5	Zhodnocení	50
4	VLASTNÍ NÁVRHY ŘEŠENÍ	51
4.1	Návrhy řešení ze SWOT analýzy	51
4.1.1	Celkové přínosy řešení ze SWOT analýzy	55
4.1.2	Finanční a časová náročnost řešení ze SWOT analýzy	55
4.2	Návrhy řešení z metody HOS	57
4.2.1	Celkové přínosy řešení z metody HOS	59
4.2.2	Finanční a časová náročnost řešení z metody HOS	59
4.3	Celkové shrnutí	60
	ZÁVĚR	61
	SEZNAM POUŽITÉ LITERATURY	62

SEZNAM POUŽITÝCH OBRÁZKŮ	65
SEZNAM POUŽITÝCH TABULEK.....	66

ÚVOD

V dnešní době se většina podniků již neobejde bez informačního systému, který je zpracován v elektronické podobě. Najdou se firmy, které stále využívají papírové zpracování, ale při porovnání efektivnosti práce jasně zaostávají právě za elektronickým. Vzhledem ke stále rostoucím nárokům v oblasti informačních technologií, je poté potřeba dbát nejen na jeho správné a užitečné využívání, ale zároveň, s množícími se útoky na data uživatelů, je nutné tyto systémy dostatečně zabezpečit.

Ke správnému výsledku je nejdříve důležité přesně a jasně identifikovat, co od daného systému očekáváme a až poté hledat a vymýšlet konkrétní řešení. Výsledné naimplementované řešení se musí dále sledovat a měnit v důsledku aktuálních trendů v oblasti informačních systémů a také podle požadavků pro co nejefektivnější chod firmy. Při nedostatečném vývoji se může firma začít potácet s až likvidačními následky kvůli nedostatečné konkurenceschopnosti.

Ve své práci budu posuzovat účinnost a hledat případné chyby informačního systému Všeobecné zdravotní pojišťovny, který spravuje firma Elso Service Brno, spol. s.r.o. V první části jsou vysvětleny základní pojmy a nastíněna problematika týkající se informačních systémů. V druhé části již přecházím k přímým analýzám tohoto systému, jejichž výsledky interpretuji ve třetí části, kde navrhuji vlastní řešení případných problémů nebo vylepšení, které by mohly vést k celkovému posunutí daného systému k lepšímu a co nejefektivnějšímu fungování.

1 VYMEZENÍ PROBLÉMU A CÍLE PRÁCE

Cílem bakalářské práce je dostatečně popsat funkčnost informačního systému Všeobecné Zdravotní Pojišťovny, který shromažďuje údaje o svých pojištěncích. (k tomuto systému mám přístup díky firmě Elso Service Brno, spol. s.r.o., která pro VZP jejich systém spravuje). Následně systém zanalyzovat a navrhnout možné změny, které by vedly k jeho lepší funkčnosti a silnějšímu zabezpečení v něm obsažených dat.

K dosažení co nejlepšího cíle nejdříve podrobně nastíním problematiku teoretické oblasti, o kterou se budu v práci opírat. Dále popíšu, jak systém firmy pracuje a co vše ke svému fungování potřebuje. Dalším krokem bude analýza současného stavu, ve které využiji metodu silných a slabých stránek a příležitostí a hrozeb (SWOT analýza) a metodu HOS. Výsledky těchto analýz shrnu a pokusím se navrhnout takové změny, které daný systém zefektivní a zabezpečí.

2 TEORETICKÁ VÝCHODISKA PRÁCE

Pro správné pochopení souvislostí popisovaných v této bakalářské práci je nutné si nejdříve nastínit celkovou problematiku v oblasti informačních technologií. V této části tedy popíšu teoretické základy, o které se bude práce opírat.

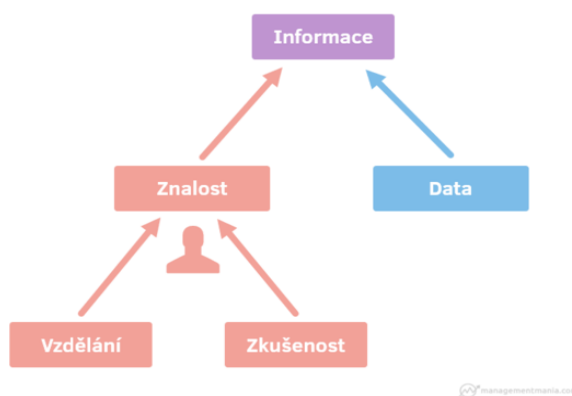
2.1 Data

Data jako takové můžeme brát za určitý stavební kámen všech vědomostí či poznatků, které po celý život získáváme. Jde o údaje, které zaznamenáme a dále je interpretujeme za pomoci vlastních znalostí, čímž z nich vytváříme informace (1).

2.2 Informace

Pojem informace má v dnešní době hned několik rozdílných definicí. Ať už je definována jako určité sdělení nebo zpráva, přes popis určité skutečnosti, která má pro jednotlivce nějaký smysl až po složitější definice popisující informaci jako energetickou veličinu. Pro smysl mé práce bych informaci definoval jako funkčně a cíleně interpretovaná data (2).

Kvalitní informace tedy musí být dobře cílená, jasná a prezentována správným způsobem tak, aby ji druhá strana přesně pochopila. V dnešní době je informace brána jako výrobní zdroj a pokládá se tedy na úroveň pracovních sil, surovin či peněz. Právě proto by se s nimi mělo dostatečně efektivně nakládat (3).



Obrázek č.1: Schéma informace (Zdroj: 4)

2.3 Proces

Proces je děj, který má přesnou trajektorii od startu až k cíli. V určitém bodě tedy začíná, přes další body prochází a v určitém bodě zase končí. Je nutné říct, že proces nemůže být nějak chaotický či neuspořádaný, vždy jde o sled událostí, které jsou prováděny s daným předpokladem a za určitým cílem. Procesů existuje nepřehledné množství napříč všemi možnými disciplínami. Všechny tyto procesy mají ale společné to, že přeměňují souhrn vstupů na souhrn výstupů pomocí jasně daných činností. Tyto výstupy se následně dají měřit a pomocí těchto měření se určuje výkonnost daného procesu (5).

2.4 Systém

Systémem se rozumí určité uspořádání jednotlivých prvků, které spolu navzájem souvisí a spolupracují. Tyto systémy se rozlišují na umělé a přirozené. Umělé systémy jsou primárně vytvořeny člověkem pro usnadnění určitých procesů často ke zjednodušení života. Přirozené systémy jsou tvořeny hlavními částmi, které nejsou nijak závislé na činnosti člověka (6).

2.5 Hardware

Za hardware se považují všechny součásti počítače, které jsou potřebné k jeho fungování a zároveň jsou i fyzicky viditelné. Patří do něj například pevný disk, paměti RAM, grafická karta či procesor (7).

2.6 Software

Software je přesný opak hardwaru, jde o programové vybavení počítače, tedy o sadu určitých instrukcí, pomocí kterých počítač může fungovat a usnadňovat práci jeho uživateli. Software vzniká programováním pomocí některého z programovacích jazyků (8).

2.7 Informační systémy

Pojem informační systém (často zkracovaný jako IS/ICT) je již delší dobu používán v odborné literatuře. *„Informační systém organizace je systém informačních a komunikačních technologií, dat a lidí, jehož cílem je efektivní podpora informačních, rozhodovacích a řídicích procesů na všech úrovních řízení organizace.“* (9)

2.7.1 Podnikové systémy

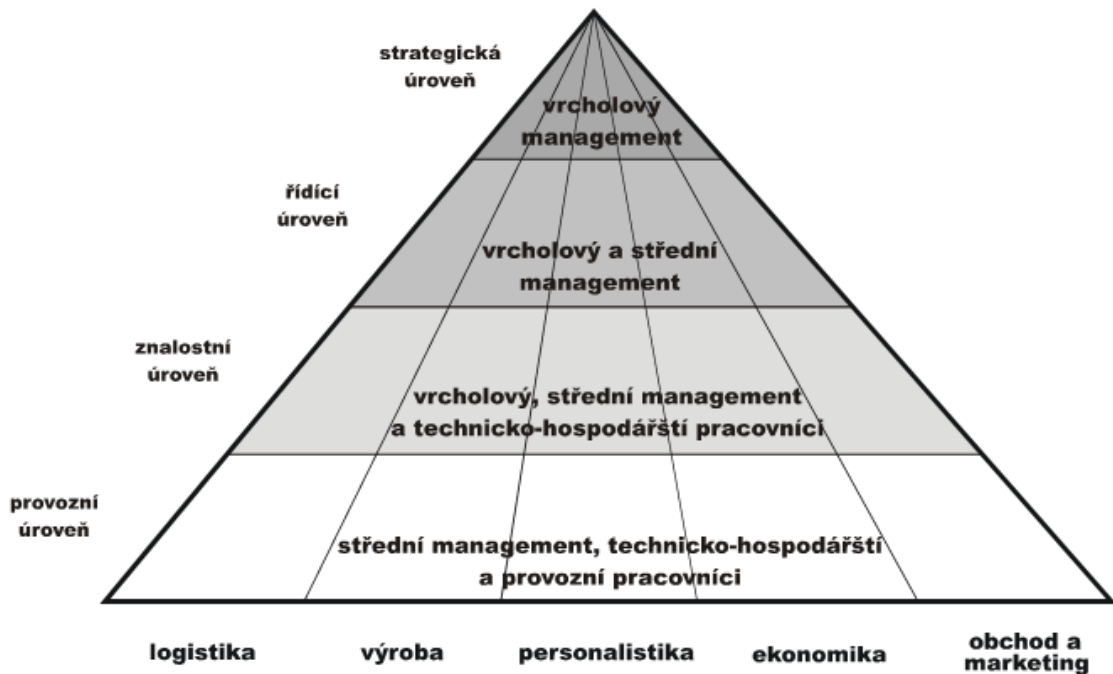
Za základní kámen, zajišťující správné fungování a růst firmy, se často udává její efektivní zpracování informací společně s vytvářením znalostní báze. Přesně tyto věci by měl zajišťovat dobrý a správně navržený podnikový informační systém. Tento systém vytvářejí lidé, kteří pomocí dostupných technologických prostředků a metodik vytvářejí z dat, které v podniku proudí, informace důležité k řízení podnikových procesů, manažerskému rozhodování a správě podnikové agendy. Je důležité si před jeho zavedením položit zásadní otázky, a to, zda daný podnik informační systém vůbec potřebuje a jak ho případně co nejlépe využít. Na tyto otázky pomůže najít odpověď strategická analýza podniku, která určí a popíše jednotlivé podnikové procesy a stěžejní faktory. Ve výsledku nastíní právě možný informační systém (10).

2.7.2 Klasifikace podnikových informačních systémů

Ve většině firmách můžeme najít hned několik organizačních úrovní, kde každá z nich potřebuje jiný přístup než ty ostatní. Za tyto úrovně se považují:

- **Provozní úroveň** – má za úkol zpracovávání informací týkajících se každodenních procesů, které podnik řeší např. realizace objednávek, nákupu, prodeje, vyplácení výplat apod.
- **Znalostní úroveň** – obsahuje veškeré aplikace podnikového informačního systému, které podporují růst znalostní báze a řídí především tok dokumentů.
- **Řídící úroveň** – kontroluje se v ní, jestli podnik správně funguje, je zde tedy potřeba shromažďovat informace o jeho činnostech k plnění administrativních úkolů a podpoře rozhodování.
- **Strategická úroveň** – tato část napomáhá vrcholnému managementu určovat dlouhodobé trendy, odhalovat očekávané změny a zjišťovat, zda je daný podnik schopný na tyto změny reagovat.

Tato klasifikace se spíše používá k teoretickému náhledu na fungování podniku, která popisuje hodnotu automatizovaného zpracování informací pro pracovníky na jednotlivých úrovních (10).



Obrázek č.2: Klasifikace úrovní podniku (Zdroj: 10)

Klasifikace, která bere v potaz více praktickou stránku věci je holisticko-procesní. Podle ní tvoří podnikový systém:

- **ERP** – typ aplikačního softwaru, který řídí a koordinuje všechny zdroje a aktivity v podniku. Automatizuje a integruje procesy, které patří v podniku k těm klíčovým (11).

ERP systémy se na trhu vyskytují ve třech možných variantách:

- **Lite ERP** – jedná se o verzi ERP, která obsahuje značně méně funkcí oproti kompletnímu ERP. Tuto verzi nejčastěji využívají malé a střední podniky. Systém je většinou obrán o maximální kapacity možných uživatelů či nepřístupnost některých modelů. Výhodou této varianty je jednoznačně nižší cena naproti tomu nevýhodou je již zmíněná limitovaná funkčnost a často není možné tyto systémy rozšířit či přejít přímo na plnou verzi (11).

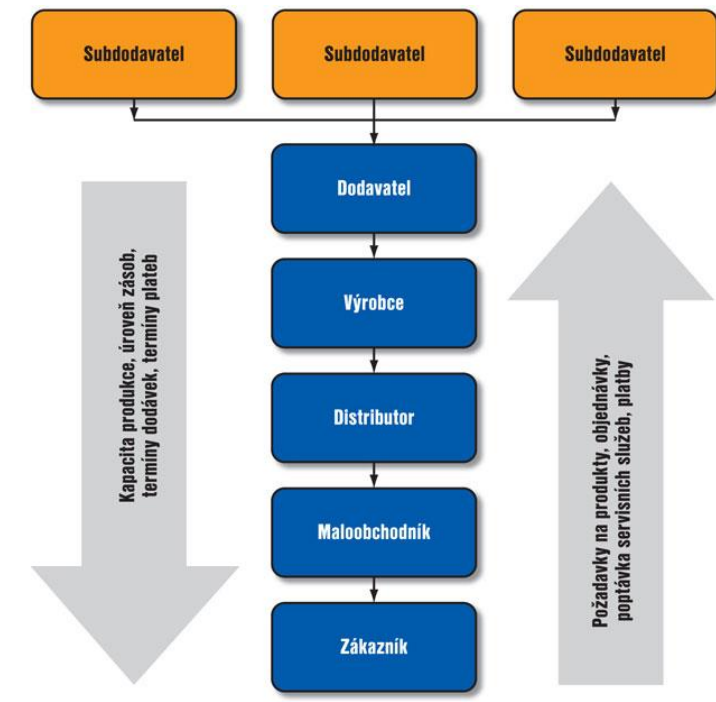
- **Best-of-Breed ERP** – tato verze je charakteristická specializací na určitý segment podnikání díky přesně navrhnutým procesům, které nejsou standartní. Tato specifická je jasnou výhodou oproti tomu má tato verze systémů často nedostatky týkající se zbytku podnikových procesů, což často vede k zavádění více systémů v rámci jedné organizace. Při využití právě většího počtu systémů, může často docházet k chybám na straně špatné komunikace mezi nimi. Zároveň tyto systémy nepokrývají celé spektrum podnikového řízení a musí tedy být často doplněny dalšími produkty či projekty (11).
- **All-in-One ERP** – tento typ obsahuje veškerou funkcionalitu ERP systému, jde tedy o velice všestranný systém. Hlavní výhodou je integrita celého systému a také spolehlivost. Ta je získána pomocí velké škály podniků, které tento systém využívá a tím nachází i jejich případné chyby. Na druhou stranu je nevýhodou často až velké množství modulů. Z toho pramení vyšší nároky na customizaci a zároveň tedy vyšší náklady na její realizaci (11).
- **ERP II (Rozšířené ERP)** – rozšířené ERP řeší integraci podniku a jeho IS s okolím směrem k zákazníkům a to ve 3 hlavních oblastech, kterými jsou CRM, SCM a BI (12).
- **CRM** – jde o řízení vztahu se zákazníky. „Jedná se o komplex technologií, podnikových procesů a personálních zdrojů určených pro řízení a průběžné zajišťování vztahů se zákazníky podniku, a to v oblastech podpory obchodních činností, zejména prodeje, marketingu a podpory zákaznických služeb.“ (12)

Strategie uplatňovaná v CRM se dělí na 3 základní koncepce:

- **Globální** – Tento typ koncepce nejčastěji využívají ty největší společnosti a korporace, které cílí na celosvětový trh. Samozřejmě se ale mohou najít i menší firmy, které této koncepci využívají na některém z menších trhů. Jejím hlavním rysem jsou jasně dané CRM procesy, které jsou řízeny shora a jednotlivé pobočky nemají možnost do nich zasahovat nebo je měnit. U této koncepce tedy není potřeba přílišná lokalizace datového modelu pro jednotlivé teritoria (výhradně se jedná pouze o jazykové lokalizace) (10).
- **Globální, lokálně uzpůsobená** – Je většinou využívána u velkých a středně velkých firem působících na trhu, jehož nabídka je sice řízena globálně, ačkoliv je zde potřeba určitá úprava dané koncepce, vzhledem ke specifickým podmínkám tohoto trhu na základě jeho lokálnosti. Tuto koncepci mohou ale také využívat firmy expandující do jiných států. Koncepce jako taková vychází z dříve zmíněné globální, která ale ke správnému fungování strategie potřebuje úpravy některých CRM procesů pro lepší využití na určitých trzích. Nemá tedy přesně daný datový model kvůli rozdílům v požadavcích na charakteristiku produktu, zákazníků a servisu (10).
- **Lokální** – Tato koncepce může být využívána u všech typů a velikostí firem či korporací. Důležitým znakem jsou jasně dané a přesně lokalizované CRM řešení pro každý lokální trh. Jsou dány jenom hlavní pravidla CRM strategie, ale každá jednotlivá pobočka si určuje postupy, pomocí kterých tyto pravidla splnit a jak dojít k co nejlepšímu využití své CRM koncepce. Záleží tedy nejvíce na práci jednotlivých poboček a jejího způsobu nakládání s daty (10).

Cílem využívání CRM je zlepšení komunikace se zákazníky v rámci celého podniku. Mělo by dostatečně zajistit, aby se při komunikaci nemuseli jednotlivé procesy opakovat, tedy aby byly všichni pracovníci dobře informováni o procesech, které již proběhly. K tomu by měla fungovat dostatečně centralizovaná databáze, která obsahuje nejaktuálnější data a je pro potřebné pracovníky dobře dostupná (12).

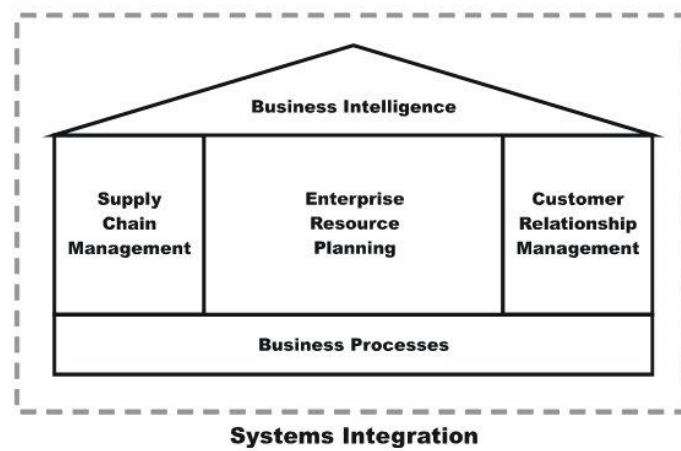
- SCM** – soubor nástrojů a procesů optimalizujících dodavatelský řetězec v rámci podniku s ohledem na koncového zákazníka. Popisuje a kontroluje celý dodavatelský řetězec s hlavním cílem zvýšení její akceschopnosti (11).
 Prakticky se jedná se o propojení dodavatele s odběratelem na bázi informačních a komunikačních technologií. Díky tomuto propojení jsou spolu oba schopni lépe spolupracovat, a to díky sdílení informací mezi sebou (12).



Obrázek č. 3: Schéma SCM (Zdroj: 13)

- BI** – soubor aplikací podporujících analytické, plánovací a rozhodovací procesy. Jejich cílem je podpořit řídicí aktivity ve firmě a zlepšovat její konkurenceschopnost (11).
 Pro podniky má hlavní funkci pro sběr a analýzu dat využitelných pro reporting, dotazování a ostatní analytické činnosti. Produkty BI přinášejí aktuální informace o všech důležitých procesech v podniku, nezávislost při jejich získávání přes více úrovní řízení a pružnost při dotazování, které není možné dopředu definovat (12).

Celý systém poté drží pohromadě systémová integrace, která má za úkol poskytovat prostředky k vytvoření a udržování na všech organizačních úrovních (10).



Obrázek č.4: Schéma ERP (Zdroj: 10)

2.8 Relační Databáze

Databází se rozumí propracovaný systém, ve kterém dochází k ukládání dat a jejich následnému zpracování. Obsahuje tedy data, která jsou propojena pomocí jasných vztahů a členěna podle předem daného relačního klíče. Tyto data se často prezentují jako tzv. atributy, tímto pojmem rozumíme hodnotu některé z entit. Pro snazší pochopení můžeme entitu chápat jako tabulku (např. Zaměstnanec), ve které jsou zaznamenávány určité atributy (např. Jméno, Věk atd.). Tyto entity musí být pro správné fungování databáze správně propojeny, čehož se docílí pomocí relací. V každé entitě je potřeba určit jasný primární klíč, který musí být jednoznačný. Tento primární klíč se poté v relaci přebírá a do druhé entity se zapisuje jako cizí klíč. Tyto relace se rozdělují na 3 typy, a to podle její kardinality (14).

- **Relace 1:1** – jedná se o nejjednodušší typ vazby. Ukazuje nám, že jednomu záznamu v tabulce odpovídá přesně jeden záznam v tabulce druhé. Tento typ relace se příliš nevyskytuje a často je jeho použití způsobena špatným návrhem celé databáze.
- **Relace 1: N** – jedná se o nejčastější typ vazby. Jeden záznam v první tabulce odpovídá několika záznamům v tabulce druhé.

- **Relace N:M** – prakticky nepoužitelná vazba. Více záznamům v první tabulce odpovídá více záznamům v tabulce druhé. Tento typ vazby se musí vždy převést na vazbu 1: N, a to pomocí spojovací tabulky, která se umístí mezi ně (15).

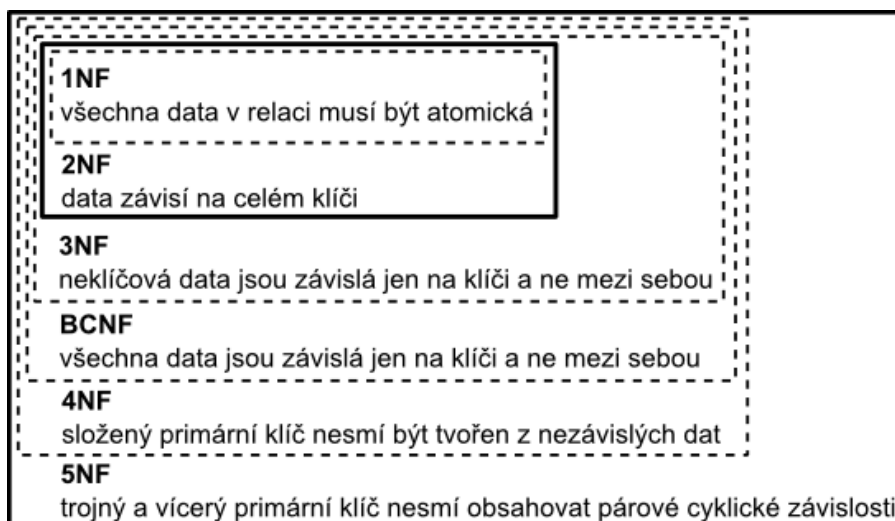
2.8.1 E-R Diagram (Entitně – Relační model)

Navrhnout kvalitní a dobře uspořádanou databázi je velmi dlouhý a důležitý proces. Po jasném určení, co v databázi chceme ukládat a k čemu ji budeme používat je dobré si navrhnout E-R Diagram. Ten graficky zobrazuje objekty a jejich vztahy v databázi. Zavádíme do něj již zmiňované entity a atributy, které mezi sebou pomocí relací spojujeme a zjišťujeme jejich kardinalitu. Toto grafické znázornění velice napomáhá perfektnímu pochopení a navržení dané databáze (14).

2.8.2 Normalizace

Pro efektivní návrh a následné fungování relační databáze je dobré ji normalizovat. Proces normalizace upravuje návrhy datových struktur tak aby byla práce s daty co nejjednodušší, lépe se s nimi manipulovalo a aby nedocházelo k tzv. redundanci dat (zbytečně se opakující data). Existuje hned několik normálních forem, které se sebou navzájem souvisí. Při porušení některé z těchto forem není datový model navržen optimálně a je dobré zvážit jeho předělání (14).

- **První normální forma** – všechna data v relaci musí být atomická což znamená, že žádný záznam v tabulce již nejde dál rozdělit.
 - **Druhá normální forma** – pokud se relace nachází v první normální formě a zároveň data závisí na celém klíči což znamená, že v tabulce nesmí být sloupec, který není závislý na primárním klíči.
 - **Třetí normální forma** – pokud se relace nachází v druhé normální formě a zároveň jsou neklíčová data závislá jen na klíči, a ne mezi sebou.
- Další normální formy jsou ukázány v následujícím obrázku (14).



Obrázek č.5: Normalizace (Zdroj: 16)

2.8.3 SQL

SQL je strukturovaný dotazovací jazyk pro manipulaci, správu a organizování dat uložených v databázi. Nejčastěji používaná dotazy jsou SELECT pro výpis dat z tabulky, DELETE pro smazání dat, UPDATE pro přepsání dat a INSERT pro vložení dat. Zároveň se však pomocí něj dá vytvářet nové tabulky společně s vazbami (17).

2.9 Informační bezpečnost

Používání informačních technologií v rámci podniku rozhodně přináší velké množství benefitů zároveň je však potřeba jejich využívání dostatečně zabezpečovat. Tyto zabezpečení by měly být komplexní s ohledem na všechny složky informačního systému (hardware, software, peopleware, data i vliv reálného světa) (3).

Vzhledem k rostoucímu trendu využívání technologií roste také počet útoků prováděných se záminkou získat data uživatelů nebo vedoucích k jinému poškození nejen uživatelů ale i celých podniků. Za aktuální hrozby lze považovat vytváření webových stránek zaměřených na krádeže hesel, spamy, malware, útoky na mobilní zařízení, krádeže identity, vývoj programů provádějící automatizované útoky a celkový nárůst zranitelnosti softwaru (3).

Útoky na informační technologie jsou nejčastěji prováděny z následujících důvodů:

- **Přerušeni nebo zničení** – dočasné nebo trvalé ukončení dostupnosti některé části informačního systému
- **Odposlech** – nepovolaný přístup k cizím informacím
- **Změna** – modifikace některé části informačního systému
- **Přidání funkcí nebo dat** – šíření dezinformací (3).

Těmto útokům lze částečně předcházet zavedením vhodných technických opatření. Zavedení přístupových karet, omezení práv uživatelů k datům, které opravdu potřebují a ochránit tok dat pomocí antivirových kontrol je rozhodně dobré zajistit. Při posouzení bezpečnosti informačního systému je však dobré brát v potaz to, že je silný pouze tak, jak je silný jeho nejslabší článek. Tímto článkem v informačních systémech je rozhodně uživatel. Proto je důležité zajistit dostatečné povědomí o informační bezpečnosti v řadách zaměstnanců (3).

Jednotliví uživatelé by si v rámci bezpečnosti měli dávat dostatečný pozor na:

- **Autentizaci** – ověřit si osobu, se kterou komunikují
- **Autorizaci** – ověřit si, že daná osoba má práva, jaká nárokuje
- **Soukromí** – zabránit jakékoliv možnosti odposlechu nebo jiné možnosti ukradnutí informací
- **Integritu** – obsah konverzace nelze nijak následně měnit
- **Neodvolatelnost** – osoba by neměla být schopná popřít psaní zpráv

Nedodržení těchto složek může mít někdy až fatální následky nejen na uživatele ale dokonce na celé firmy (3).

2.9.1 GDPR

Pojem GDPR je v poslední době slyšet snad ze všech stran. Jde o nový právní rámec, který má za úkol ochránit osobní údaje v evropském prostoru a hájit práva občanů proti neoprávněnému zacházení s jejich daty. Toto nařízení musí akceptovat všechny firmy, instituce, jednotlivci, a dokonce i online služby, které jakýmkoliv způsobem shromažďují osobní údaje. Při porušení tohoto právního rámce hrozí obrovské pokuty, které mohou

být často pro některé firmy dokonce až existenční problémy. V evropské unii je účinné od 28. května 2018 a u nás nahrazuje současnou právní úpravu o ochraně osobních dat. Veškeré firmy, kterých se toto ustanovení týká museli právě do května 2018 upravit své informační systémy tak, aby byly v souladu s GDPR. U nemalého počtu firem tento krok vyvolal velmi negativní pocit. Hlavním přínosem by však měla být vyšší ochrana osobních údajů, které se v poslední době stávají stále větším terčem útoků (18).

2.10 Nástroje analýzy

Pro správné posouzení firmy nebo informačního systému existuje velké množství analýz, které využívají různorodé metody pro zjištění současného stavu. Jako 2 hlavní bych označil SWOT a HOS.

2.10.1 SWOT analýza

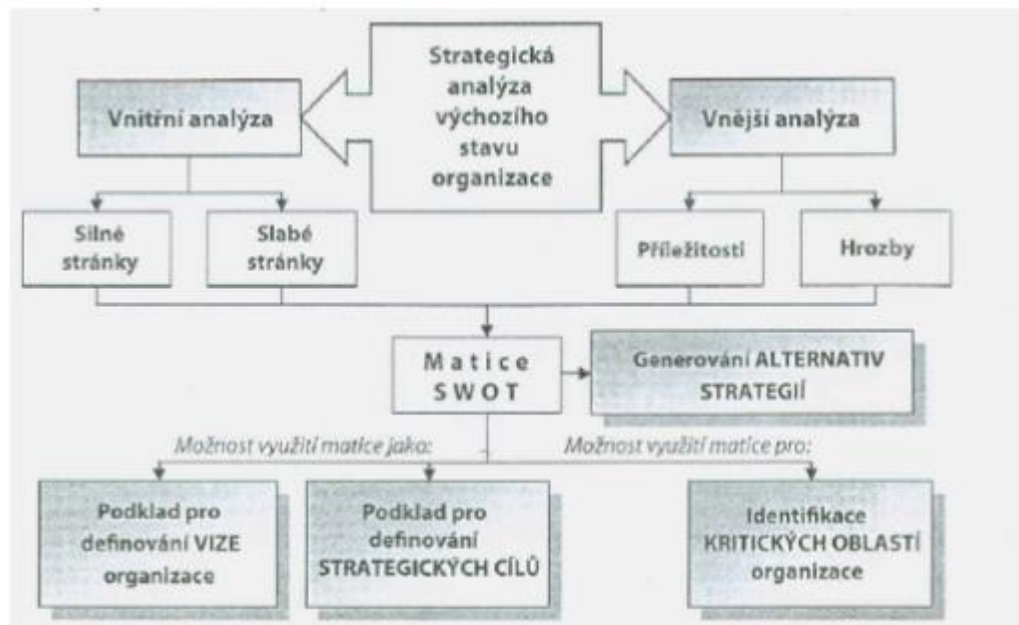
Jedná se o typ strategické analýzy podniku, jejíž název je akronymem pro vnitřní silné (strengths) a slabé stránky (weaknesses) organizace a příležitosti (opportunities) a hrozby (threats) identifikované ve vnějším prostředí organizace. Výsledkem by měla být tzv. SWOT matice, určená pro vytvoření strategie organizace právě na základě již zmíněných čtyřech pilířích.

Pro správné provedení SWOT analýzy je důležité rozlišit faktory podle toho, jestli patří do vnitřního nebo vnějšího prostředí. Při špatném zařazení jednotlivých faktorů může být výsledná analýza nepřesná.

Při analyzování vnitřního prostředí se hodnotí silné a slabé stránky organizace, které vymezují vnitřní faktory efektivnosti ve všech významných oblastech. Stěžejním faktorem je především to, zda zdroje a možnosti organizace odpovídají působení vnějšího prostředí na organizaci (19).

Za faktory vnějšího prostředí se rozumí oblasti, které nemůže sama organizace nijak ovlivnit, jsou tedy na organizaci nezávislé a působí na ni z prostředí mimo ni. Výsledkem těchto faktorů je buď hrozba nebo příležitost (19).

SWOT analýza je naprosto bezpředmětná, pokud je použita pouze jako argument, že daný tým pro přípravu strategie využil některý z nástrojů, ale její výsledky nejsou ve strategii nijak použity. Je dobré si před provedením analýzy určit, co jejím provedením chceme zjistit, a ne tedy pouze kopírovat postupy, které při jiných problémech fungovaly (19).



Obrázek č.6: SWOT schéma (Zdroj: 19)

2.10.2 Metoda HOS

Tento typ analýzy hodnotí jednotlivé složky informačního systému, u kterých hledá slabé stránky snižující celkovou úroveň systému. Metoda HOS tedy hledá nejslabší články systému, jelikož vychází z úvahy, že je systém dobrý tak jako jeho nejslabší část. Posuzuje tedy úrovně jednotlivých oblastí systému vzhledem k jeho ostatním složkám. Právě nevyváženost těchto složek totiž vede k neefektivnímu využívání systému (20).

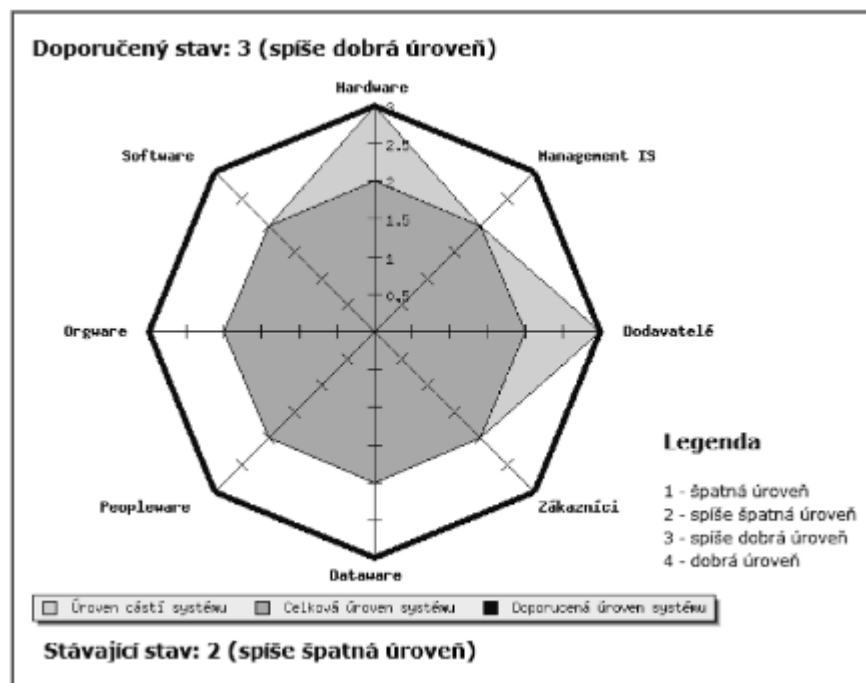
Na základě dlouhodobého výzkumu v oblasti informačních systémů metoda HOS posuzuje 8 klíčových částí informačního systému:

- **Hardware** – technické vybavení firmy
- **Software** – programové vybavení firmy
- **Orgware** – doporučené postupy ve firmě

- **Peopleware** – uživatelé informačního systému
- **Dataware** – práce s daty v systému
- **Customers** – zákazníci využívající informační systém
- **Suppliers** – dodavatel informačního systému
- **Management** – řízení v rámci informačního systému

Jednotlivé oblasti se v rámci prvního kroku hodnotí pomocí škály jako 1 – špatná, 2 – spíše špatná, 3 – spíše dobrá a 4 – dobrá. Toto hodnocení je většinou prováděno na základě dotazníků obsahujících několik kontrolních otázek ke každé ze zmíněných oblastí. Výsledky jsou poté prezentovány v rámci procentuálního zisku (20).

Výsledky jsou následně znázorněny pomocí soustavy čtyř os. Při vyváženém systému by měly všechny osy mít stejné hodnocení, nebo nanejvýš tři z nich by se měly odlišovat o maximálně jeden hodnotící bod. Doporučený stav systému se poté odvíjí od jeho důležitosti, kterou mu daná firma přikládá (20).



Obrázek č.7: Ukázka výsledku metody HOS (Zdroj: 20)

3 ANALÝZA PROBLÉMU A SOUČASNÉ SITUACE

Tato část práce slouží k popisu společnosti VZP a jejího informačního systému, který následně budu také podrobněji zkoumat. Zároveň zde i krátce popíši firmu Elso Service, která tento systém spravuje a díky níž k němu mám přístup a potřebné informace.

Dále v této části také provedu SWOT a HOS analýzu informačního systému, z jejichž výsledků budu vycházet v další části práce.

3.1 Společnost Elso Service Brno, spol. a.s.

Tabulka č.1: Základní údaje o firmě Elso Service (Zdroj: 21)

Název:	Elso Service Brno, spol. s.r.o.
Sídlo:	Koliště 92/21c, 602 00 Brno
IČO:	61854671
Počet zaměstnanců:	Cca 25
Předmět podnikání:	Dodávka řešení v oblasti informačních řešení



Obrázek č.8: Logo Elso Service (Zdroj: 21)

Brněnská firma Elso Service patří do větší skupiny Elso Group, která se zabývá dodávkou hardwaru ale i softwarových řešení již od roku 1993. Samotná firma se poté hlavně zabývá vývojem kompletních IT řešení na klíč. Při tomto vývoji používá softwarový nástroj JIRA, který dokáže plánovat průběh práce a zároveň pomáhá odhalit chyby a problémy. Firma v této době zaměstnává okolo 25 zaměstnanců, mezi kterými figurují zkušení analytici, techničtí i systémový specialisté a programátoři. Těmto zaměstnancům se firma snaží zajišťovat velké množství certifikací v systému Oracle, ve kterém pracuje a je i jeho zlatým partnerem. Díky tomu je firma schopná navrhnout, co nejlepší řešení vzhledem k individuálním přáním zákazníků. Mimo tyto celkové řešení také nabízí konzultace jak systémového, tak i technického charakteru. Mezi nejznámější odběratele

této firmy patří společnosti Hewlett-Packard, díky níž mají zaměstnanci k dispozici vždy nejnovější modely notebooků této značky, a VZP, u které firma dodává klíčové části informačního systému pro zpracování a vyúčtování zdravotní péče včetně jeho správy (21).

Právě tento systém budu v mé práci posuzovat.

3.2 Všeobecná zdravotní pojišťovna

Tabulka č.2: Základní údaje o VZP (Zdroj: 22)

Název:	Všeobecná Zdravotní Pojišťovna České republiky
Sídlo:	Orlická 2020/4, 130 00 Praha 3 - Vinohrady
IČO:	41197518
Počet zaměstnanců:	4000–4999
Předmět podnikání:	Činnosti v oblasti povinného sociálního zabezpečení



Obrázek č.9: Logo Všeobecné zdravotní pojišťovny (Zdroj: 22)

Všeobecná zdravotní pojišťovna patří k nejužší špičce v rámci českého systému veřejného zdravotního pojištění. Byla založena na počátku roku 1992 a funguje na trhu tedy více než 25 let. V současné době má téměř 6 milionů klientů a z tohoto pohledu je v České republice ta největší. Jejich hlavním úkolem je hrazení zdravotních služeb, které potřebují jejich klienti, platící si pojistné. Za jeden rok se jejich vynaložené peníze na léčbu klientů pohybují kolem 180 miliard a každým rokem stoupají. Vzhledem k jejímu

postavení v konkurenci ostatních pojišťoven se může chlubit tím, že má uzavřenou smlouvu s více než 96 % praktických lékařů a 40 tisíci zdravotnických zařízení. Po celé zemi se nachází kolem 190 poboček, a proto se jedná i o nejdostupnější pojišťovnu v České republice. V jejím čele stojí ředitel, který je zvolen a případně odvolán správní radou (22).

3.2.1 Konkurence

Pro lepší pochopení situace VZP na trhu zdravotních pojišťoven je dobré zmapovat její konkurenci. Na základě zpráv ministerstva zdravotnictví působí v České republice dalších 6 zdravotních pojišťoven:

- *Vojenská zdravotní pojišťovna (VoZP)*
- *Česká průmyslová zdravotní pojišťovna (ČPZP)*
- *Oborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví (OZP)*
- *Zaměstnanecká pojišťovna Škoda (ZPŠ)*
- *Zdravotní pojišťovna ministerstva vnitra ČR (ZP MV)*
- *Revírní bratrská pokladna, zdravotní pojišťovna (RBP)*

VZP dle dostupných údajů k 31.12. 2018 má registrovaných přes 57 %, z předpokládaných 5,9 milionu pojištěnců systému všeobecného zdravotního pojištění. To ji zajišťuje velmi dobré postavení na tomto trhu a s přehledem se dá říct, že mu značně dominuje. V následující tabulce jsou porovnány jednotlivé pojišťovny na základě některých ze souhrnných ukazatelů.

Tabulka č.3: Porovnání pojišťoven (Zdroj: Vlastní zpracování)

	VZP	VoZP	ČPZP	OZP	ZPŠ	ZP MV	RBP
Počet pojištěnců (v tis.)	5 926	700	1 244	731	143	1 307	430
Počet pojištěnců na zaměstnance	1 624	1 647	1 947	1 864	1 835	2 029	1 876
Kumulovaný rozdíl příjmů a výdajů (2014-2018) na jednoho pojištěnce (Kč)	2 828	-100	-527	1 789	797	-492	-891
Peněžní prostředky na 1 pojištěnce (Kč)	2 624	1 370	2 574	3 937	4 580	2 879	3 335

Vzhledem k údajům v tabulce č. 3 můžeme vidět již zmíněnou dominanci VZP v počtu pojištěnců. Dalšími většími pojišťovnami v tomto ohledu jsou potom Zdravotní pojišťovna ministerstva vnitra a Česká průmyslová zdravotní pojišťovna. Rozhodně se ovšem nejedná o stejnou velikost jako VZP, ani součet pojištěnců těchto dvou pojišťoven se stále nepřibližuje VZP. Ukazatel počtu pojištěnců na jednoho zaměstnance ve zkratce ukazuje, jak daná pojišťovna dokáže vyřizovat požadavky klientů. Čím méně je pojištěnců na zaměstnance, tím více prostoru může každý z nich získat bez toho, aby vznikaly zdlouhavé prostoje u ostatních. Znovu zde nejlépe dopadla VZP, což je i přes velký počet klientů patřičný úspěch.

Další ukazatel nám ukazuje to, jak dokáží jednotlivé pojišťovny hospodařit. Vzhledem k tomu, že je tento rozdíl v příjmech a výdajích přepočtený na jednoho pojištěnce se zde ztrácí jakékoliv výhody postavení na trhu a dá se tedy mluvit o velmi relevantním porovnávajícím údaji. Opět nejlépe dopadla VZP, která je pouze s Oborovou zdravotní pojišťovnou a Zaměstnaneckou pojišťovnou Škoda v kladných hodnotách. Poslední vybraný ukazatel mapuje to, kolik finančních prostředků má pojišťovna ihned k dispozici na jednoho pojištěnce. Zde nejlépe dopadly Zaměstnanecká pojišťovna Škoda

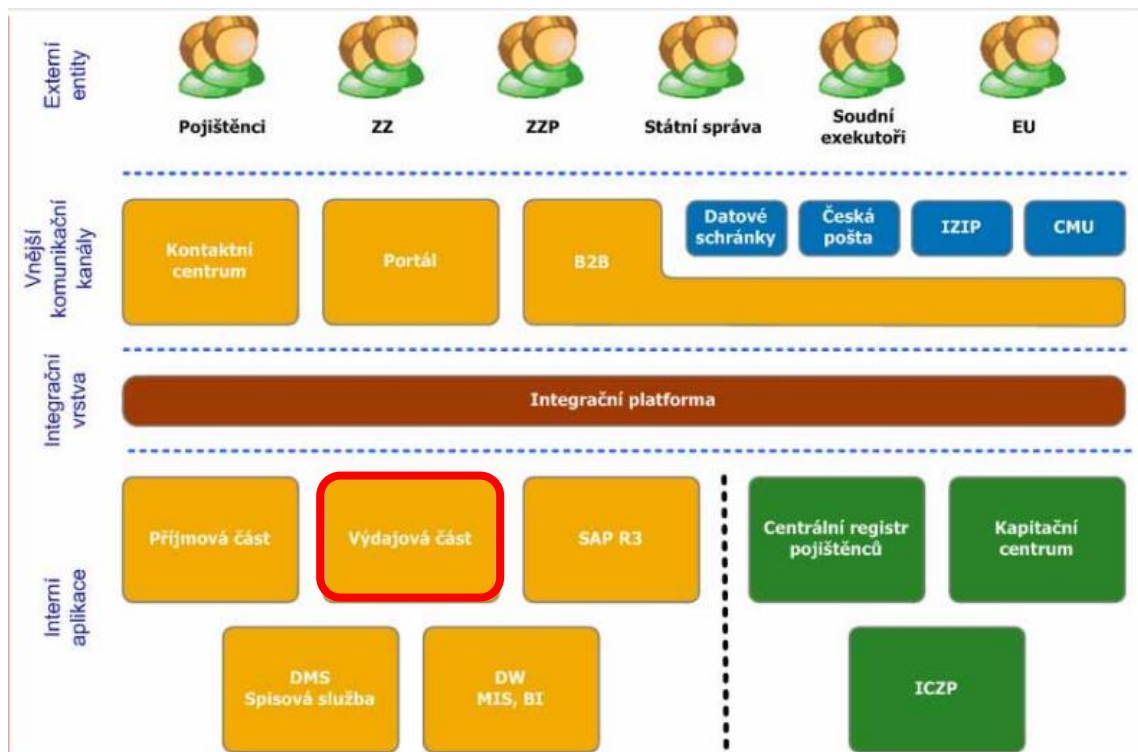
a Oborová zdravotní pojišťovna, vůči kterým VZP značně ztrácí, nicméně na tom není nejhůře.

Z pohledu těchto vybraných ukazatelů můžeme vidět, že VZP je jasný gigant na poli pojišťovnictví v ČR. Své postavení si drží již delší dobu a vzhledem její plošné podpoře a široké síti poboček se nemusí tolik konkurence bát, přestože ostatní pojišťovny pomalu rostou v počtech pojištěnců má VZP stále více než polovinu z nich na své straně. Samozřejmě ale musí pokračovat v dostatečně dobré kvalitě svých služeb.

3.3 Informační systém VZP

Informační systém VZP je velice rozsáhlý, a to nejen z pohledu jeho architektury, ale zároveň i z důvodu zpracovávání obrovského objemu dat. Systém jako takový má množství funkcí, které ve výsledku vedou k usnadnění a urychlení práce zaměstnanců, a tedy podporu vnitřního chodu celé organizace. Mezi hlavní funkce rozhodně patří výběr pojistného od pojištěnců, a to především kontrola těchto úhrad ve správný čas a v případě problému, usnadnění jejich vymáhání. Neméně důležitým je také z druhé strany hrazení a kontrola poskytnuté péče jejím klientům prostřednictvím zdravotnických zařízení. Tyto údaje zaznamenává do svých databází a následně je analyzuje a sestavuje statistické přehledy. Další funkce, které musí systém zajišťovat jsou mu dané přímo zákonem. Jedná se o *správu centrálního registru pojištěnců*, který zaznamenává základní údaje o všech pojištěncích veřejného zdravotního pojištění, *vedení informačního centra zdravotního pojištění*, *registr zdravotnických zařízení*, jehož úkolem je vést kompletní přehled o poskytovatelích zdravotní péče v ČR s podrobnými údaji, a *provoz kapitačního centra*, které řeší kapitační platby.

Jedná se o modulární systém s centralizovanou architekturou, který obsahuje velké množství komponent, aplikací a modulů, spojených přes integrační platformu. Jednotlivé aplikace jsou vyvíjeny na míru, tedy pouze pro potřeby VZP.



Obrázek č.10: Schéma architektury IS VZP (Zdroj: Dokumenty firmy Elso Service)

Páteř systému tvoří interní systém VZP dělicí se na příjmovou a výdajovou část. Příjmová část má na starosti přijímání úhrad od poskytovatelů a příjem pojistného. Výdajová část řeší evidenci a vytváření podkladů pro správný výpočet úhrady, o který se následně taky stará. Výdajová část se ještě rozděluje na online a off-line část. Právě off-line částí výdajové oblasti se budu ve své práci podrobně zabývat, protože se jedná o stěžejní oblast celého informačního systému a vzhledem k velikosti celého IS a rozsahu mé práce, nejde podrobně popsat IS úplně celý.

Online část výdajové oblasti přebírá podklady pro zpracování jednotlivých dávek a dokladů přebraných od poskytovatelů zdravotní péče. Stará se o ně už od jejich nahrání do systému až po celkové uzavření jejich zpracování. Tomuto procesu se říká tzv. primární nacenění. Zároveň také v této části probíhají kontroly a revize zadaných údajů, řeší se tu storna, proplácení lázeňských a jiných forem ozdravné péče a také se jedná o určitý přístupový bod pro značnou část uživatelů.

Většina těchto procesů probíhá v tzv. pracovní oblasti, která řeší kompletní zpracování všech typů dávek, a to až po jejich uzavření a následnou archivaci. Po uzavření zpracování dat se tyto soubory posílají do Archivní cache a tím současně i do off-line části.

Off-line část se dělí na dva další celky, a to repozitory a archiv. Repozitory má za úkol především poskytování dat pro úlohy provozované v off-line části. Data tu jsou uchovávána v rozmezí cca 8 let. Tento celek je plněn společně s převáděním dat do archivní cache v online části. Archiv shromažďuje starší data, která již nemusí být obsažena v repozitory a nejsou tedy již potřebné pro prováděné úlohy.

V rámci této off-line části probíhají tedy veškeré hlavní výpočty v oddílu repozitory. Jedná se o 3 hlavní celky zpracování nebo úloh:

- **Úhradové** – vyúčtování nemocnic, ambulantních specialistů či následné péče
- **Bonifikační** – program kvality péče AKORD
- **Regulační** – regulace nemocnic či praktických lékařů

Následně se zde nachází určité podpůrné úlohy, které mají za úkol sesbírat potřebná data a ty následně zprostředkovat dalším úlohám. Dalším typem jsou úlohy statistické. Ty vypočítávají a porovnávají data, které následně musí VZP předávat dalším institucím (statistický úřad, ministerstvo zdravotnictví atd.).

Komunikace mezi jednotlivými částmi nebo aplikacemi probíhá podle toho, jak velký objem dat se přenáší. Při běžném případě sdílení dat mezi dvěma aplikacemi v prostředí VZP využívá integrační platforma technologii Advanced queuing (jedná se o technologii Oracle). Přenos spočívá v tom, že zdrojová aplikace zasílá zprávy obsahující potřebná

data do fronty na integrační platformě, ta zjistí, komu je zpráva určena a přepošle data do fronty cílové aplikace. Cílová aplikace si poté data z fronty zpracuje podle potřeby.

V případě přenosu většího množství dat, je však tento způsob velmi neefektivní, jelikož je k tomuto přesunu potřeba velké množství zpráv, které zahlťují integrační platformu a celý proces se značně ztěžuje a zpomaluje. Právě pro tento typ přenosů se využívá framework SDI (silná datová integrace), který umožňuje efektivní a rychlý přenos většího množství dat. Tímto způsobem jsou následně přenášena data mezi online a off-line částí.

3.3.1 Uživatelé

Veškeré interní aplikace informačního systému využívají pouze pracovníci VZP, kteří jsou co nejlépe poučeni k jeho používání vzhledem k bezpečnosti dat pojištěnců. Tito pracovníci mají přidělené role jejichž koncept je rozdělen na 3 hlavní větve, které se mohou prolínat:

- **Business role**
- **Typová role**
- **Aplikační role**

Business role, které definuje VZP, jsou spjaty s business procesy ve firmě a mohou být nadřazeny některým částím IS. Tato role může obsahovat větší množství typových rolí v rámci jednoho systému.

Typové role jsou logické celky sdružující aplikační práva podle požadované funkcionality. Tyto celky opět vytváří VZP, kde je jejím podkladem návrh ze strany dodavatele IS. Typové role mohou sdružovat několik rolí aplikačních. Aplikační role jsou děleny na ty, které mají právo pouze údaje prohlížet (nemají tedy právo je nijak měnit či modifikovat) a role aktualizací, resp. výkonné jenž mají právo data vkládat, měnit nebo s nimi, jakkoliv pracovat. V rámci systému existují i speciální oprávnění k určitým akcím, které může provádět jen malý okruh pracovníků.

3.3.2 Hardware a Software

Celý systém pracuje nad databázemi Oracle s využitím aplikačního rozhraní Oracle Forms a Oracle Reports, které již nejsou bohužel podporovány Oraclem. Potřebné aplikace jsou následně vyvíjeny v programovacím jazyku Java.

Hardwarové vybavení týkající se užívaných serverů je řešeno on premise, to znamená, že servery jsou fyzicky vlastněny a firma se musí o tyto servery starat a spravovat je (druhé možné řešení je pomocí cloudu, kde jsou servery hostovány a nemusí je firma sama spravovat). Základem serverové infrastruktury, která je centralizovaná a provozovaná v rámci datových center, jsou servery nebo i jejich systémy pracující na architektuře procesoru x86. Firma není vázána na jediného konkrétního výrobce. Hlavními požadavky na servery jsou dostatečná rozšiřitelnost, maximální flexibilita a vysoká dostupnost. Jednotlivé servery nebo systémy jsou propojeny pomocí sítě LAN a vybaveny co nejkvalitnějšími nástroji pro správu. Pro případ možné virtualizace je hardware management propojen s virtualizační vrstvou. Tyto servery jsou typu rackmount (19“ provedení, které sedí do standardních racků) a v rámci datových center jsou umístěny v rackových skříních o velikosti 42 unitů. Jejich napájení se odvíjí od spotřeby jednotlivých zapojených zařízení. Kvůli lepšímu zabezpečení a správě dat je zaveden SAN (Storage Area Network), do kterého jsou v jednotlivých datových centrech zapojeny diskové pole. Tyto diskové pole jsou pro potřebnou kapacitu rozšiřovány (nejsou nakupovány další pole). Tato SAN infrastruktura obsahuje mimo zmíněná pole ještě všechny významné servery a zálohovací knihovny. Každé aplikaci je přidělena kategorie, určující její důležitost:

- **A++** - aplikace jakékoliv ze skupin A (A++, A+, A) jsou tzv. business kritické a technologické aplikace, které mají vysokou důležitost v rámci celého systému a jejich výpadek může mít zásadní dopad na celý provoz systému. Tyto aplikace jsou provozované na části infrastruktury, na kterou nemají dopad případné výpadky fyzických komponent. Provoz probíhá v rámci dvou lokalit jedna je brána primárně jako aktivní a druhá záložní, která se využívá k testování, anebo v případě výpadku první lokality. Třída A++ pracuje aktivně v režimu aktiv/aktiv na obou lokalitách současně, takže v případě výpadku aplikace funguje stále a nedojde k téměř žádnému zpoždění jejího chodu, pouze může mít tento

výpadek vliv na její výkonnost. Typicky je tato skupina prováděna pomocí geografického Oracle RAC clusteru v kombinaci s HP ServiceGuard a Oracle ASM, data jsou následně zrcadlena pomocí Veritas Volume Managera.

- **A+** - aplikace aktivně pracují v režimu aktiv/aktiv jedné lokality a v případě problému, mohou být manuálně přepnuty na lokalitu druhou. V případě výpadku se aplikace přepne do druhé lokality automaticky, po dobu nutnou pro přepnutí se stává daná aplikace dočasně nedostupnou a tento výpadek může mít opět vliv na její výkonnost. Typicky je využívána lokální Oracle RAC cluster společně s HP SG a Oracle ASM. Zrcadlení spravuje technologie HP Continuous Access XP.
- **A** – aplikace pracují v režimu aktiv/pasiv mezi oběma lokalitami a funguje poté totožně jako třída A+. Typicky poté využívá geografický HP SG cluster s nakonfigurovaným failover aplikačním balíčkem pro Oracle databázi. Zrcadlení dat je prováděno prostřednictvím technologie HP Continuous Access XP, Veritas VM, MirrorUX.
- **B** – aplikace třídy B nepatří mezi nejkritičtější aplikace systému a mají tedy nižší nároky na zajištění jejich dostupnosti. Tyto aplikace již neleží v části infrastruktury, která eliminuje hardware výpadky jejich částí. Data také nejsou zrcadlena do druhé lokality a není tedy využíváno clusterového řešení. Dostupnost je zajišťována prostřednictvím serveru, na kterém daná aplikace běží.

Jednotlivé pracovní počítače jsou vybaveny operačním systémem Windows 7 Enterprise, který je plně kompatibilní s používanými aplikacemi. Na počítačích se nachází Microsoft Word a Excel ve verzi z roku 2010. Ochrana je zajišťována antivirovým programem od firmy Kaspersky přesněji Kaspersky Endpoint Security, který je řízený centrálně. Obsahuje veškeré potřebné prvky ochrany od antiMalware přes firewall až po Device control. Na vybraných pracovních počítačích se nachází systém pro šifrování disků a souborů (Endpoint Encryption, Area Guard Neo). Počítače nelze bez souhlasu oprávněné osoby přenastavit, avšak instalování nových programů není nijak kontrolováno. Připojení tiskáren je řešeno převážně přes tiskový server z důvodů větší bezpečnosti. Veškeré počítače mají stejnou adresářovou strukturu pro lepší přehlednost. Připojení přes VPN je řešeno klientem Cisco AnyConnect Secure Mobility a nachází se pouze na vybraných notebookech. Tyto notebooky dodává firma HP.

3.3.3 Bezpečnost

Vzhledem k velké citlivosti uchovávaných dat v databázi je bezpečnost spojená nejen s přihlašováním do systému, ale i následnou prací v něm, velmi kontrolována a vyžadována. Je nařízeno striktní dodržování zákona o ochraně osobních údajů a zákona autorského. Bezpečnost se poté řídí směrnicí, kde vše, co není výslovně povoleno je zakázáno. Tyto pravidla platí pro všechny systémy, aplikace, procesy, zaměstnance, uživatele apod. V případě nutnosti nasazení nové komponenty IS do provozu je nutné provést test zranitelnosti, a to pomocí nástroje NESSUS (nástroj hledá potencionální bezpečnostní díry) či nezávislou externí firmou, která provede penetrační test. Veškeré informace shromažďované v rámci systému mají definovanou míru citlivosti, ta je odvozena od důležitosti dané informace pro společnost, případně zákonem. Tato kategorie určuje, jak se může s informací zacházet. Každá taková informace musí mít také přiděleného vlastníka, kvůli zodpovědnosti a dohledatelnosti v případě špatného zacházení. Vlastník má povinnost zodpovídat za definování pravidel přístupu a zacházení s informací. Citlivost informace také definuje délku držení informace v systému. Při práci s nimi musí být jasně identifikováno kdo, kdy, kam a co provedl.

Přístup jednotlivých uživatelů do systému je prováděn přes přidělenou identitu uživatele, která je uchovávána v Active directory (adresářová služba od Microsoftu pro uložení identit). Identity jsou poté řízeny Identity managementem. Každý uživatel si vytvoří heslo do systému, které musí splňovat velmi přísné požadavky. Musí mít minimální délku 8 znaků z kombinace alfa-numerických symbolů, nesmí se vztahovat k práci nebo osobnímu životu (např. jména rodinných příslušníků, značka vozidla atd.) a nesmí používat slova, která jsou samostatně obsažená ve slovníku. Složitost hesla odpovídá citlivosti informace, čím větší citlivost = tím větší požadovaná složitost. Heslo musí být následně uchováno v tajnosti (nesmí být zapsáno v čitelné podobě) a měněno periodicky (maximální doba platnosti jednoho hesla je 90 dní). Při nezměnění hesla v dané době, se účet automaticky blokuje a pro jeho zpětné zprovoznění je nutné kontaktovat administrátora systému. V případě podezření možnosti prolomení hesla je nutné jej ihned změnit.

System má implementovanou ochranu proti útokům na hesla uživatelů. V případě několika neoprávněných přístupů dojde k automatickému uzamčení daného účtu, následné odemknutí je řešeno prostřednictvím administrátora systému. Zároveň je tento mechanismus navržen tak, aby nedošlo k hromadnému zamykání více účtů a tím k odepření služby.

Do systému se také přihlašují uživatelé pomocí VPN. Na tento typ připojování má VZP vlastní normy a směrnice, které platí pro všechny interní i externí subjekty. Je zavedena tzv. dvou faktorová autentizace. Nejdříve musí být žadatelovi přidělen certifikát od VZP (pro potřeby VPN VZP neakceptuje jiné certifikáty než své vlastní), dále je mu přiděleno uživatelské jméno a vyžádáno heslo (stejně podmínky jako u běžných uživatelů). Všechna zařízení, která jsou do sítě připojována musí být zabezpečena minimálně uživatelským jménem a heslem. Veškeré externí připojení je sledováno a zaznamenáváno, tudíž je vše dohledatelné.

3.3.3.1 Zálohování

Jedním z nejdůležitějších bezpečnostních požadavků v takové databázi, jako má VZP je zálohování dat. V případě výpadku by bez zálohování mohlo dojít k velmi citelné ztrátě, která by mohla vést k velkým časovým průtahům a problémům. Zálohování dat je řešeno speciálním softwarem, který běží ve všech datových centrech. Fyzicky jsou data ukládána na dvojici knihoven ve dvou datových centrech. Proces zálohování jako takový probíhá křížem, a to vždy z datového úložiště v jedné lokalitě na pásku v lokalitě druhé. Mechanismus je totožný pro všechny aplikace a systémy.

3.3.4 Práce v systému

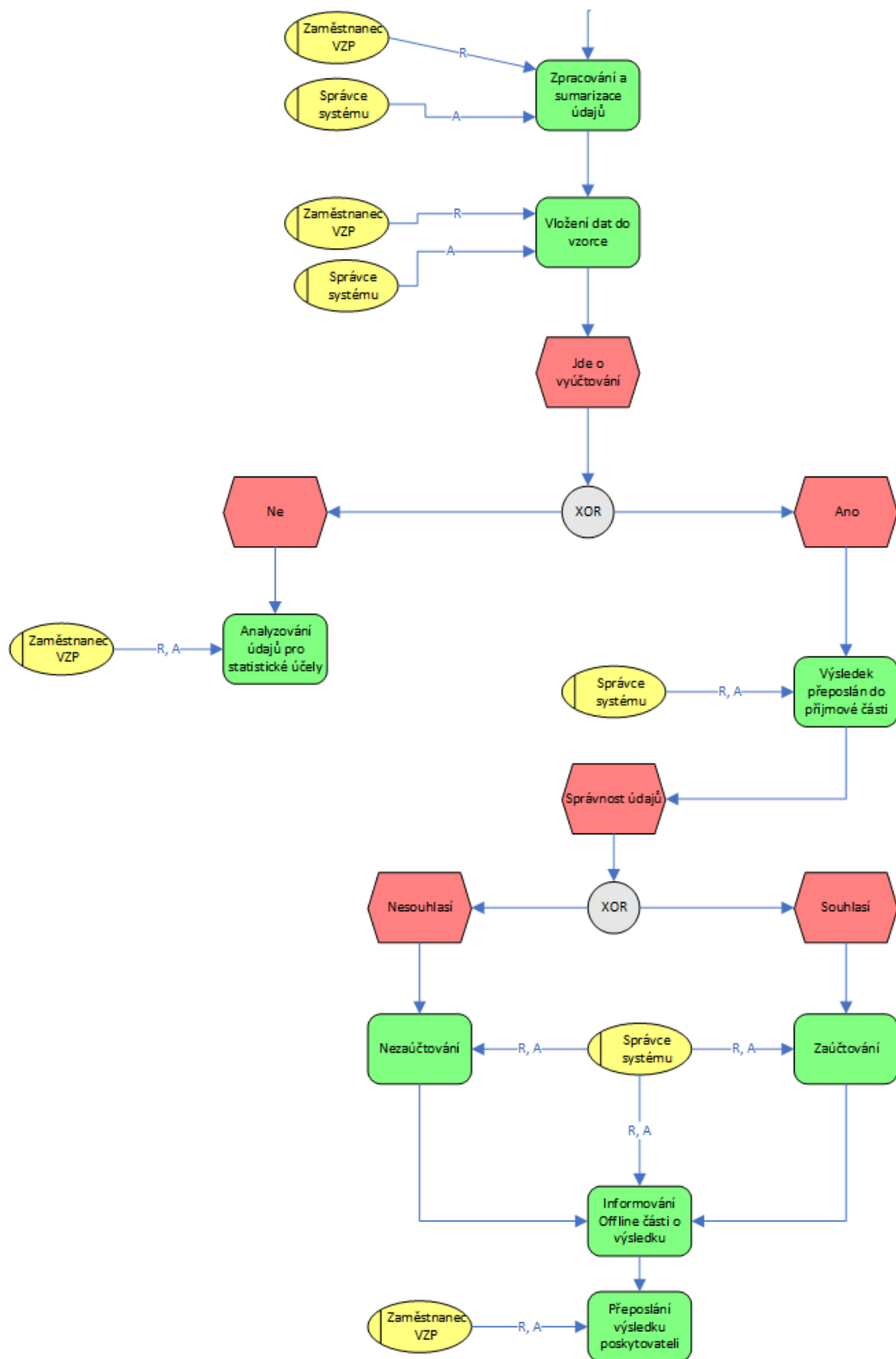
Pro lepší pochopení toho, jak systém pracuje se pokusím napsat průběh běžného zpracování dat v systému. Představme si situaci, že jako pojištěnec VZP jdu ke svému obvodnímu lékaři na prohlídku (lékař má normálně uzavřenou smlouvu s VZP).

Při příchodu lékař zjistí pomocí kartičky pojišťovny či z již zaznamenaných údajů, to že jsem pojištěncem VZP a provede potřebné vyšetření. Následně vše zaeviduje ve svém rozhraní na počítači (které je univerzální pro všechny pojišťovny) a vyřeší potřebné další kroky (výpis receptu, posláni odběrů, doporučení ke specialistům atd.). Tyto data poté nejčastěji elektronicky odešle do systému VZP (přenášení na médiu či v papírovém

zpracování se v dnešní době již moc neděje). Tyto údaje se v systému VZP zaevidují v online části výdajového úseku s určitým obdobím VZP (na základě měsíce předání do VZP). Tato část provede validaci a kontrolu přeposlaných dat. Jestli je vše v pořádku, tak se data přeposílají do online výkonné části, kde se potřebné úkony ocení podle platných číselníků a tento doklad je připraven pro přenos do off-line části. Toto ohodnocení se provádí každý měsíc prostřednictvím tzv. bodových uzávěrek, které oceňují právě podle aktuálních ceníků. Po této uzávěrce je doklad odeslán právě do off-line části, kde se s ním dále pracuje a následně se archivuje. V off-line části se provádí zpracování dokladů, a to většinou za jeden rok pro vytvoření podkladů pro platby. Cílem je tedy sumarizovat data úkonů, které poskytovatelé péče za zadané období provedli. Tento proces probíhá tak, že se nejdříve ve formuláři nastaví parametry potřebné sumarizace. Následuje spuštění sběru dat uchovaných v repozitory což je většinou časově nejnáročnější část celého procesu. Po shromáždění těchto dat je na řadě daný výpočet, který má za úkol data sumarizovat tak aby mohli vstoupit do vzorce výsledné úhrady pro jednotlivá zařízení (lékař, nemocnice atd.). Vypočtené částky se následně přeposílají přes integrační platformu do příjmové části, kde dochází buď k zaúčtování či nezaúčtování na základě správnosti dat o čemž je off-line část informována poslaným vyrozuměním přes integrační platformu. Off-line část následně informuje poskytovatele zdravotní péče posláním výsledku tohoto vyúčtování. Tento proces je znázorněn na následujícím zjednodušeném EPC diagramu, pro lepší pochopení (viz obrázek 11 a 12).



Obrázek č.11: EPC diagram procesu v rámci IS část 1 (Zdroj: Vlastní zpracování)



Obrázek č.12: EPC diagram procesu v rámci IS část 2 (Zdroj: Vlastní zpracování)

V případě provádění tohoto zpracování dat pouze pro analytické či statistické účely je vynechán celkový proces vyúčtování.

Vzhledem k tomu, že se jedná o naprosto obrovské množství zpracovávaných dat, je délka celkové zpracování v rámci několika hodin. Je tedy možné tyto zpracování přesně naplánovat na určitý čas nebo je samozřejmě spustit hned. V některých případech, kdy je spuštěno více zpracování naráz může totiž dojít k problému, že se tyto zpracování budou o některá potřebná data „hádat“, právě proto je tu možnost nastavení startu každého zpracování pomocí systému spouštění zpracování. Bohužel zde schází systém, který by řešil určitou prioritizaci jednotlivých procesů, což by rozhodně pomohlo jejich správě.

3.3.5 Správa systému

Systém spravuje externí firma Elso Service, která je dodavatel IS. Firma spolupracuje a komunikuje se service deskem VZP. Vzájemná komunikace se koná prostřednictvím SD operátorů obou stran. VZP zasílá firmě emaily, kde jsou sepsány servisní požadavky. Externí firma si tyto požadavky projde a zhodnotí, v případě rozumných a uskutečnitelných požadavků je přijme a problémy poté vyřeší, v druhém případě požadavky odmítne s potřebným odůvodněním. Následně externí firma informuje VZP o průběhu servisu a případně o problémech v řešení. Veškeré zásahy do systému musí být průběžně zalogovány, kvůli případnému dohledání příčin budoucího problému.

Elso Service zpracovává požadavky na servis v systému JIRA. Tento systém dokáže plánovat a následně monitorovat průběh zpracování požadavků. Požadavky od VZP mají přiřazenou závažnost, od které se odvíjí jak čas, tak i způsob řešení (viz. Tabulka č. 4).

Tabulka č.4: Závažnosti požadavků (Zdroj: Vlastní zpracování)

Závažnost požadavku	Potřebná reakce
Blokující	<i>Reakce, vyřešení do 24 H</i>
Kritický	<i>Reakce, vyřešení do 2 pracovních dní</i>
Zásadní	<i>Reakce, vyřešení do 10 pracovních dní</i>
Drobný	<i>Reakce, vyřešení do 20 pracovních dní (Někdy i více pokud řešení přímo nespěchá)</i>
Dotaz	<i>Reakce, odpověď do 5 pracovních dní</i>
Změna	<i>V případě drobnosti se řeší v rámci supportu, jinak probíhá proces schvalování – nacení se podle pracovních, připraví se nabídka s popisem řešení a celkovou cenou a předá se ke schválení VZP – pokud se schválí tak se realizuje jinak se odloží, nebo úplně zruší</i>

3.4 Analýzy

Pro správné posouzení informačního systému využijí analýzu SWOT, kterou provedu společně s jedním ze zaměstnanců, který se o informační systém stará, a také analýzu HOS, kterou stejný zaměstnanec podpořil vyplněním potřebných dotazníků na stránce <https://www.zefis.cz/>, která je určena pro audity efektivnosti a bezpečnosti informačních systémů, ke kterému právě využívá analýzu HOS.

3.4.1 SWOT analýza IS

Pro dobré popsání aktuální situace ohledně informačního systému je dobré zjistit jeho silné a slabé stránky a zároveň možné příležitosti a hrozby (viz tabulka č.5).

Tabulka č.5: SWOT analýza IS (Zdroj: Vlastní zpracování)

Silné stránky	Slabé stránky
<p>Modulární systém na míru</p> <p>Dobrý support</p> <p>Know-how dodavatele</p> <p>Schopnost rychlé a solidní inovace</p>	<p>Nepodporovaná aplikační platforma</p> <p>Hardwarová náročnost</p> <p>Softwarová náročnost</p> <p>Uživatelská náročnost</p> <p>Chybějící interaktivní nápověda</p> <p>Nemožnost stanovení priorit u zpracování</p> <p>Nedůsledná kontrola práce uživatelů</p>
Příležitosti	Hrozby
<p>Rozšíření zpracování o pojištěnce EU</p> <p>Uživatelský náhled (formulář) zobrazující probíhající procesy</p> <p>Rozšíření tiskového subsystému (stanovení priorit tisku)</p> <p>Formulář pro modelaci úhrad</p> <p>Optimalizace procesů v rámci IS</p>	<p>Rodné číslo jako identifikátor pojištěnce v IS</p> <p>Přílišná logika ve formulářích</p> <p>Možnost instalace SW na koncová zařízení</p> <p>Uchovávání citlivých dat na koncových zařízeních</p> <p>Nevzdělanost uživatelů</p>

3.4.1.1 Silné stránky

Nejvýraznější silnou stránkou informačního systému VZP je jeho modularita. Systém je zároveň vyvinutý na míru, a to přináší dobře vyvinuté aplikace přesně přizpůsobené dané problematice. V případě problému není příliš velký problém některý model přidat či pozměnit, vše je jen otázkou peněz. S tím souvisí i další silná stránka, a to dobrá podpora v případě řešení problému. Dodavatelská firma zná systém velmi dobře a díky dobré vzájemné komunikaci může ihned přispěchat s řešením. Takže rychlá a efektivní podpora při řešení nových požadavků, dotazů nebo chyb umožňuje dobrou kvalitu celého provozu.

3.4.1.2 Slabé stránky

Nej slabší stránkou celého systému je zajisté jeho aplikační platforma. Běží na Oracle Forms a Oracle Reports. Tyto dvě platformy bohužel nejsou nadále podporované od Oracle, což v některých konkrétních případech může znamenat až neřešitelné problémy. Vzhledem k velkému toku dat v rámci systému se dá očekávat, že potřebné procesy potřebují co nejkvalitnější techniku. Z tohoto důvodu je systém velmi hardwarově náročný a některá zpracování mohou trvat až několik hodin. S tím jde ruku v ruce i náročnost softwaru, na něhož jsou požadavky taky velmi vysoké. V současné době je systém při některých procesech až nepřehledný a uživatel, který se přesně nevyzná v dané problematice, může napáchat velké škody. Uživatelská náročnost je tedy vysoká a je potřeba vyškolit zaměstnance tak, aby se v systému vyznali. V případě problému systém neobsahuje interaktivní nápovědu a uživatel je odkázán pouze na sáhodlouhé příručky, což může vést k dlouhým prostojeům. Při běžném provozu může zároveň probíhat větší množství zpracování, což by ani nebyl tak velký problém. Ten ale nastává při absenci určení priorit jednotlivých zpracování. Tato funkce v systému absolutně chybí a není tedy možné zpracování, které je pro firmu důležité vyřídit přednostně. V neposlední řadě se v rámci systému dostatečně nekontroluje práce jeho uživatelů. To může v některých případech znamenat velké problémy.

3.4.1.3 Příležitosti

VZP v současné době vede záznamy nejen o klientech z České republiky ale i o pojištencích z Evropské unie. Systém má ale všechny zpracování omezena pouze na pojištěnce právě z České republiky (v databázi typ pojištění = 1, cizinci mají typ pojištění = 4), přitom může provádět zpracování i v rámci cizinců. Toto rozšíření by rozhodně celkové efektivitě IS pomohlo. Při již zmíněné možnosti probíhání více zpracování zároveň, by bylo dobré systém rozšířit o nástroj, který by ukazoval, jaké zpracování zrovna probíhají a zároveň, co v současné době není možné zjistit, kolik času pro jednotlivá zpracování zbývá do konce. Tento nástroj by vedl mnohem lepší přehlednosti těchto procesů a k efektivnějšímu plánování jejich spouštění. VZP musí provádět velké množství hromadného tištění na svých tiskárnách. Tento hromadný tisk ovšem vede subsystém, který není dostatečně funkční. Jeho vylepšení by ulehčilo práci a zajistilo možnost nastavení priorit jednotlivých tisků, což může v některých případech hrát velmi závažnou roli. Některé procesy v systému trvají velmi dlouho, a proto by byla dobrá jejich optimalizace a případná lepší modelace některých z nich, aby nevyžadovali a nezpracovávali zbytečné údaje.

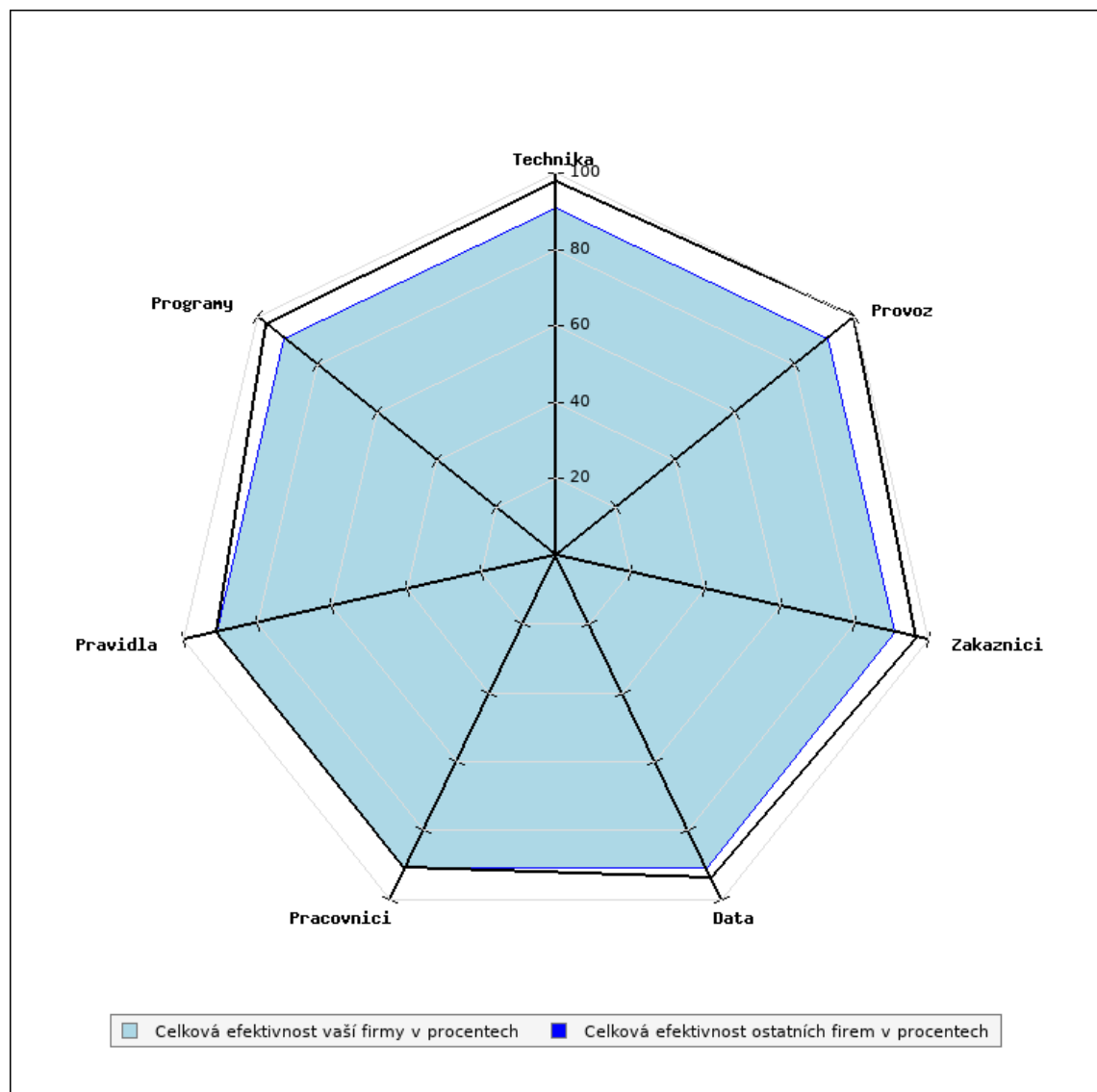
3.4.1.4 Hrozby

Systém pro práci s jednotlivými uživateli bere jako identifikátor jejich rodné číslo. Vzhledem k citlivosti dat, které databáze obsahuje, by měl být identifikátorem spíše automaticky přidělené číslo, které takto není přímo spojeno s danou osobou (i vzhledem k GDPR). V tomto případě lze dohledat všechny záznamy pomocí rodného čísla. Vzhledem k současnému nepodporování aplikační platformy Oracle Forms a Reports se objevuje ve formulářích příliš logiky. To znamená, že v některých formulářích dochází přímo k výpočtům a bylo by lepší tyto výpočty provádět až na úrovni databáze, ne přímo ve formulářích. V případě nahrazení aplikační platformy by poté výměna byla mnohem jednodušší. Další hrozbou je, že firma dovoluje uživatelům instalování aplikací na svůj počítač bez toho, aby byly řádně zkontrolovány, to v některých případech může vést k útokům na data prostřednictvím různých virů nebo může dojít k problémům ohledně licencí některých nelegálně stažených programů. Na těchto počítačích jsou zároveň uchováвана některá citlivá data, se kterými daný uživatel pracuje. Vzniká zde tedy hrozba ukradení těchto dat, když si uživatel nedává potřebný pozor na to, jak se svým počítačem

zachází. Všechny tyto hrozby poté vznikají z toho důvodu, že zaměstnanci nejsou dostatečně vzděláni v oblasti bezpečnosti a tím vystavují citlivá data nebezpečí.

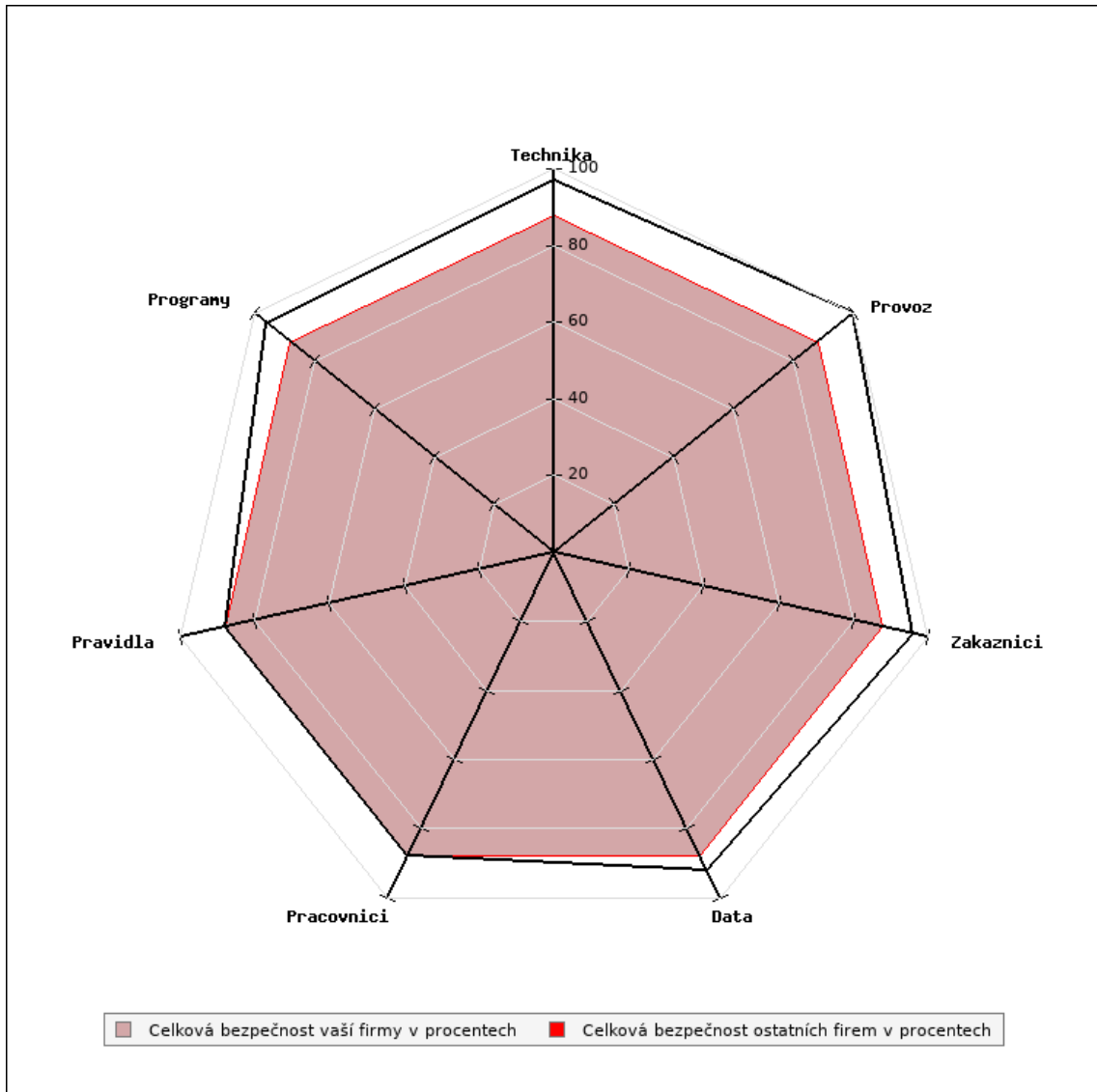
3.4.2 HOS analýza IS

Analýza HOS hodnotí informační systém z pohledu jeho efektivnosti a bezpečnosti. Z grafu výsledku efektivnosti můžeme vidět, že je systém na vysoké úrovni a všechny části jsou dostatečně vyrovnané. Celková efektivnost dosáhla 91 %, což je velmi dobrý výsledek. Vzhledem k velikosti a důležitosti systému se to dalo očekávat.



Obrázek č.13: Efektivnost systému podle HOS (Zdroj: 23)

Z pohledu bezpečnosti systém získal 88 %. Jedná se tedy opět o velmi dobrý výsledek. Vzhledem k tomu, že je výsledek znovu vyrovnaný ve všech oblastech, tak je systém i z pohledu, že každý systém je tak silný jako jeho nejslabší článek, velmi dobře zabezpečený.



Obrázek č.14: Bezpečnost systému podle HOS (Zdroj: 23)

3.4.2.1 Zjištěné nedostatky

Přes velmi dobré celkové výsledky se samozřejmě objevily určité chyby či hrozby, které by mohly v celkovém důsledku systém velmi oslabit, a proto je dobré jim věnovat dostatečnou pozornost. Nedostatky byly zjištěny na základě vyplněných dotazníků na stránce <https://www.zefis.cz/>.

- **Chybějící, nebo špatně dodržovaná bezpečnostní pravidla**

Základem dobrého fungování nejen informačního systému ale i celé firmy je správné nadefinování pravidel, které vedou k co nejlepší úrovni bezpečnosti. Zavedení špatných procesů nebo nedostatečná kontrola jejich dodržování může vést až ke kritickým problémům s obrovskými dopady na data v systému. Nedávání dostatečného důrazu bezpečnosti může mít i ten důvod, že firmě nepřináší její kontrola žádný zisk, ale pouze náklady. Následky takového jednání potom firma zjistí až při tom, když problém nastane.

- **Pracovníci mohou instalovat programy na své počítače**

Povolení pracovníkům instalovat vlastní programy sebou nese dvě zásadní hrozby, co se těchto programů týče. Pracovníci nemusí dávat dostatečný pozor na to, jestli aplikace, kterou instalují, je z její originální distribuce a že se nejedná o legální, licencovaný produkt. V takovém případě poté můžou nastat velké právní problémy, právě ohledně licencí. Tyto nelegální programy poté taky mohou obsahovat určité viry nebo špionážní software, což je v případě práce s citlivými daty velmi nebezpečné.

- **Nejsou zálohovaná data na počítačích pracovníků**

Data, se kterými pracovníci zacházejí, mohou být v případě výpadku ztraceny, a tím mohou vznikat časové prodlevy. Proto je dobré zvážit nejen zálohování systémových dat jako takových ale i těch na počítačích pracovníků.

- **Špatně nastavené pracovní postupy**

Při zavedení špatných či nedostatečných pracovních postupů se může firma dostat do velkých problémů. V rámci informačního systému, to může vést ke špatným nebo neaktuálním datům. Tyto postupy tedy musí být jasně definovány.

- **Nastavení přístupových práv**

Přístupová práva u systémů jako má například VZP, jsou naprosto stěžejní. Je nutné je nejen dobře rozdělovat a aktualizovat, ale v případě postupu zaměstnance na jinou pracovní roli upravit tak, aby měl vždy jen ty potřebné k provádění jeho práce. Zároveň je nutné taky oprávnění zrušit při ukončení pracovního poměru. Zaměstnanci vždy poukazují na práva, které jim chybí, ale už ne na ty, které jim zbytečně přebývají.

- **Nejsou nastavena pravidla práce s daty zákazníků**

V současné době, kdy je zákon GDPR skloňován snad všude, kde se zaznamenávají určitá data, je potřeba nastolit správná pravidla týkající se této práce. Tyto pravidla musí jasně určovat, kdo a jak může s daty pracovat a musí se jasně hlídat jejich dodržování.

- **Neprobíhají periodická bezpečnostní školení uživatelů IS**

Žádný systém nebude pracovat na 100 % pokud ho nebudou spravovat dobře informovaní pracovníci. Proto jsou školení ohledně všech bezpečnostních ale i funkčních opatření nezbytná. Tyto školení by zároveň měli probíhat s určitou periodičností.

- **Odpovědnost pracovníků za data**

Pro nejaktuálnější data v systému je důležité jim přiřadit odpovědného vlastníka, který se o tyto data bude starat.

- **Chybí pravidla pro zavedení dat do systému**

Je dobré zavést pravidla ohledně zadávání nových dat do systému, a to z důvodu přehlednosti a určité pravidelnosti. Zároveň je důležité zadávat tyto data ve správné formě, jinak jsou téměř k ničemu.

- **Není vytvářeno bezpečnostní povědomí pracovníků**

Nejen, že je důležité dbát na již zmíněná bezpečnostní pravidla systému, ale také na bezpečnost práce zaměstnance na svém počítači i mimo své pracoviště. Zásady, jak se chovat na internetu, reagovat na podezřelé e-maily nebo nedocházet od přihlášeného počítače, je důležité dodržovat.

- **Špatně stanovená zodpovědnost pracovníků v procesu**

Za každý proces, který v rámci systému probíhá musí být jasně definovaná odpovědná osoba. Hlavním důvodem je dohledání viníka v případě problému,

zároveň tato osoba zodpovídá a dělá vše pro to, aby daný proces probíhal co nejkvalitněji. Tato osoba musí být vždy pouze jedna, v případě více osob je tu riziko toho, že na sebe budou navzájem spoléhat a daný proces ani nezačne.

- **Riziko ztráty a zneužití dat**

Počítače pracovníků obsahují citlivá data, hesla do systému VZP mají velmi striktní pravidla nejen pro podobu hesla, ale zároveň vyžadují jeho časté měnění. To sice zajišťuje dobrou bezpečnost, ale není to vše, co může cílová data chránit. Je nutné šifrování těchto dat, aby v případě ztráty zařízení, nemohl nikdo nepovolaný tyto data přečíst a zneužít je. Proto je nutné již zmíněné dobré podvědomí pracovníků o celkové bezpečnosti a zároveň i předpokládat možné problémy a těm předcházet například šifrováním.

- **Bezpečnostní hrozba z přístupu na internet**

Je dobré zvážit, zda pracovníci potřebují ke své práci přístup k internetu. Při jeho používání totiž vzniká hrozba útoku na data. Jestli tedy zaměstnanec ke své práci internet nepotřebuje je lepší ho vůbec nezavádět. V opačném případě je nutné udělat vše pro to, aby případný útok nemohl nic poškodit.

3.5 Zhodnocení

Z analýz informačního systému VZP jsme zjistili, že je systém celkově dobře navržený, a hlavně dostatečně vyrovnaný. Jeho efektivita se pohybuje nad 90 %, což je velmi dobrý výsledek a bezpečnostně je na necelých 90 % takže procesy v něm jsou navrženy velmi obstojně. Hlavními zjištěnými problémy jsou nedostatečná vzdělanost jeho uživatelů z čehož může hrozit ztráta některých citlivých dat. V systému se těchto dat nachází velké množství, a tak jsou některé procesy velmi zdlouhavé a nenapomáhá tomu fakt, že je systém velmi uživatelsky náročný a orientace v něm může být obtížná. Aplikační platformy, na kterých systém stojí, již nejsou dále podporovány a bylo by dobré zvážit jejich nahrazení, nebo upravení systému tak, aby se výpočty prováděli na úrovni databáze. Dalším problémem je používání rodného čísla jako indikátoru což je zvoleno velmi nešťastně. Celkově ale systém pracuje velmi dobře a až na zmíněné nedostatky není potřeba větší počet změn.

4 VLASTNÍ NÁVRHY ŘEŠENÍ

V této kapitole budu vycházet z výsledků předcházejících analýz informačního systému. Navrhnou řešení, které by mohlo nalezené problémy vyřešit a zlepšit tím celkový obraz IS.

4.1 Návrhy řešení ze SWOT analýzy

Analýza SWOT odhalila určité hrozby a příležitosti týkající se systému VZP. Zároveň také ukázala, že mezi nejsilnější stránky systému bezesporu patří jeho modularita, čímž se systém stává velmi schopným při reagování na potřebné změny a také že VZP může plně spoléhat na podporu od svého dodavatele, který systém spravuje dostatečně dlouhou dobu na to, aby mu plně porozuměl. Následné řešení by měly systém celkově vylepšit a posílit bezpečnost uložených dat a vyřešit již zmíněné hrozby.

- **Aplikační platforma**

Vzhledem k problému, že aplikační platformy Oracle Forms a Reports, již nejsou dále podporovány od Oraclu, bylo by dobré zvážit případnou změnu aplikační platformy. Bohužel v dnešní době nejspíše neexistuje podobná platforma jako zmíněné Forms a Reports, která by byla kompatibilní s Oracllem. Řešení, které se poté nabízí je využít předělání celé aplikace přes programovací jazyk Java. Toto řešení by ale znamenalo vysoké náklady a je také velmi časově náročné. I přes to, že v současné době přestal Oracle tyto platformy podporovat, je možné, že v budoucnu se k nim vrátí, právě z důvodu složitého nahrazování jejich funkcí. Jako nejlepší řešení této situace se jeví to, že by se systém postupně začal připravovat na případnou změnu celé platformy, a kdyby se Oracle definitivně rozhodl skončit s podporou Forms a Reports, předělat veškeré aplikace právě pomocí jazyka Java.

- **Přesunutí výpočtů na úroveň databáze**

Vhledem k problému s aplikační platformou je dobré právě pro případ přechodu na jinou, přesunout všechny výkonné funkce na úroveň databází. V současném stavu systému se většina logiky těchto výpočtů nachází přímo ve formulářích a aplikačním prostředí. Pro lepší funkcionalitu je důležité přesunout veškerou logiku právě přímo do databází. V následném případě, kdy bude muset být celý

system předělán a logika by byla přímo ve formulářích, by bylo toto předělání prakticky nemožné nebo přinejmenším zbytečně složité.

- **Interaktivní nápověda**

Uživatelská náročnost celého systému je velmi vysoká, dokonce dochází i k případům, že z důvodu těžké orientace v systému uživatelé špatně zachází s jednotlivými funkcemi, což může vést až k nebezpečným ztrátám dat. Jedním z možných řešení je zavedení interaktivní nápovědy v rámci celého systému. V současném stavu je k dispozici pouze množství příruček, které jsou ovšem příliš obsáhlé a hledání v nich právě potřebné rady se stává velmi zdoluhavým procesem. Vytvoření interaktivní nápovědy, která bude přímo reagovat na přesné dotazy uživatelů může práci v systému zjednodušit a tím i celý systém zefektivnit.

- **Prioritizace zpracování**

V systému probíhá velké množství zpracování potřebných dat. V případě delšího zpracování má uživatel možnost jej naplánovat tak, jak je potřeba (například delší zpracování naplánovat přes noc). Problém spočívá v tom, že jednotlivým zpracováním nelze nastavit prioritu. Některé ze zpracování jsou však důležitější než ostatní a systém by měl právě ty provádět přednostně. Nabízí se tedy vytvoření určitého systému prioritizace, ve kterém by každý uživatel mohl tuto prioritu nastavit. Zároveň by potom vedoucí pracovník, mohl sledovat průběh zpracování a měl by mnohem větší přehled o tom, co je nejdůležitější.

- **Probíhající zpracování**

Dalším problémem ohledně lepší přehlednosti probíhajících zpracování je, že nikde nelze zobrazit, kolik času zbývá do dokončení určitého zpracování. Absence této informace způsobuje problémy uživatelům, kteří se právě o zpracování starají. Dobré by bylo tedy vytvořit formulář, který by ukazoval podrobnější informace o probíhajících zpracováních, v tomto formuláři by se také mohla zobrazovat již zmíněná priorita tohoto zpracování, a to by vedlo lepšímu plánování procesů a práci by to zefektivnilo.

- **Kontrola práce uživatelů**

Nejčastějšími problémy v informačních systémech obecně, jsou chyby jeho uživatelů. V informačním systému VZP nedochází podle provedených analýz k dostatečné kontrole práce jeho uživatelů. Je potřeba zavést takové postupy, které

dovolují co nejméně chyb a předcházejí možným únikům dat. Systém sledování toho, co pracovníci dělají je určitě dobrým řešením, i přes to, že z pohledu zaměstnanců není příliš vítaným. V takto velkém a důležitém systému, obsahujícím obrovské množství citlivých dat musí ale být pracovní postupy hlídány velmi striktně. Zároveň je také důležité přidělovat zaměstnancům odpovědnost za svou práci, která je dohledatelná v případě problému.

- **Zpracovávání údajů cizinců**

Systém v současné době obsahuje, jak údaje svých českých pojištěnců, tak ale i zároveň údaje o cizincích v rámci Evropské unie. Veškeré zpracování mají však omezení dat striktně danou pouze na české pojištěnce. U každého klienta je v databázi nastaven typ pojištění (pro ČR je tato hodnota = 1, pro cizince = 4). Vzhledem k tomu, že databáze již tyto údaje shromažďuje bylo by dobré s nimi i dále pracovat. Změna by měla nastat v jednotlivých formulářích pro spouštění daných zpracování. Ze striktně zadané hodnoty 1 v políčku typ pojištění, by mělo být možné zvolit, zda nechceme zpracovávat jenom cizince případně všechny pojištěnce dohromady. Tato změna by rozšířila možnost analyzování dat a mohla by přinést lepší a podrobnější výsledky. Zároveň by toto zpracování nemuselo probíhat další stranou.

- **Tiskový sub-systém**

VZP tiskne velké množství dokumentů, dopisů atd. každý den. Bohužel nemají v rámci svého systému tyto procesy dostatečně hlídané a nastavitelné. Z toho důvodu poté dochází k situacím, kdy zaměstnanec potřebuje vytisknout něco důležitého, ale musí čekat, než se dotiskne například dávka dopisů pro pojištěnce což může trvat i několik hodin, zároveň nemá šanci zjistit, co vše je ve frontě a jak dlouho by to mělo ještě trvat. Vylepšení tiskového subsystému by tento problém vyřešilo. Šlo by jasně vidět co se tiskne, kolik času do konce zbývá a zároveň by měla přibýt i možnost určení priorit u tisku, tak aby nejdůležitější dokumenty nemusely stát ve frontě.

- **Změna identifikátoru**

System v databázi pracuje s rodným číslem klientů jako identifikátorem. Toto řešení je hned z několika důvodů nešťastné. Případní uživatelé systému se mohou velmi lehce dostat k citlivým datům jednotlivých klientů, a to pouze po zadání jejich rodného čísla, které v dnešní době už není takový problém zjistit. Proto je jediným možným řešením přiřazovat pojištěncům automatické identifikační číslo, a s tím následně pracovat v rámci aplikací. Toto řešení je s ohledem na velikost celé databáze velmi složité a zdouhavé ale není zde jiná možnost, jak tyto data lépe uchránit. Je tedy nutné všem pojištěncům přiřadit identifikační číslo a v celé aplikaci již pracovat s tímto identifikátorem, místo nyní používaného rodného čísla. Zároveň by bylo dobré ostatní údaje pro zaměstnance skrýt, aby z databázi nemohl vyčíst zbytečně moc údajů, ale pouze ty, které ke své práci potřebují.

- **Lepší kontrola zaměstnaneckých cílových zařízení**

Zaměstnanci nemají nijak kontrolované instalování programů na počítače, ze kterých se připojují do systémů. Tím vzniká riziko instalace nebezpečných programů, které by mohly obsahovat viry nebo špionážní software. Tato možnost by měla být zakázána a veškerý software instalovaný na pracovní stanice, by měl kontrolovat určený vedoucí pracovník. Nastavení této kontroly povede k vyšší bezpečnosti dat v systému a zamezí instalaci nelegálních nebo nelicencovaných programů. Zároveň je potřeba zakázat stahování dat ze systému, právě do těchto počítačů. K tomu bych doporučil zavedení cloudového řešení, které je rozhodně bezpečnější variantou. Není totiž potřeba aby data, se kterými uživatelé pracují, musela být fyzicky na jejich počítačích.

- **Lepší vzdělanost zaměstnanců**

V neposlední řadě je velkým problémem nedostatečně vzdělávání pracovníků se systémem. Pracovníci dostanou pučení ohledně bezpečnostních postupů při nástupu do firmy. Problém je v tom, že se tyto znalosti dále netestují a neobnovují. Pro to je potřeba zavést pravidelné bezpečnostní schůzky, na kterých budou uživatelé systému poučováni ohledně bezpečnosti a zároveň nejnovějších aktualizací systému. Tyto schůzky musí být povinné a vedeny dostatečně erudovaným pracovníkem v dané oblasti.

4.1.1 Celkové přínosy řešení ze SWOT analýzy

Tyto zmíněná řešení by měla vést k podpoření silných stránek informačního systému a zároveň k eliminaci stránek slabých. Celkově by mělo dojít k lepší funkcionalitě v případě nalezení lepší aplikační platformy nebo alespoň ke snížení závislosti systému na dané již nepodporované platformě. Další řešení zajistí lepší uživatelskou přehlednost v rámci celkového fungování v systému. Přínosem v oblasti bezpečnosti údajů by mělo být zavedení nového identifikátoru, který již nebude spojován přímo s rodným číslem a zároveň zlepšení kontroly uživatelů systému nejen při práci v něm ale zároveň s ohledem na chování na svých pracovních stanicích. Při provedení všech navržených změn se stane systém efektivnější, bude se v něm lépe orientovat a data klientů budou více zabezpečena.

4.1.2 Finanční a časová náročnost řešení ze SWOT analýzy

Navržené změny jsem po probrání s dodavatelskou firmou, u které získávám o systému informace, zhodnotil nejen z pohledu jejich časové náročnosti, ale i z pohledu ekonomického. Časová náročnost byla odvozena pomocí porovnání s časy analogických prací. Následné finanční ohodnocení bylo přepočítáno podle sazby 5 000 Kč za MD (ManDay = člověkodén). Tento údaj není stejný jako u dodavatelské firmy z důvodu zachování určité diskrétnosti. Celkový čas řešení zahrnuje konzultace, analýzy, implementaci, testování, upgrady a aktualizaci uživatelských příruček. Nezahrnuje školení cílových zaměstnanců. Vše je zobrazeno v následující tabulce, včetně řešení, které řeší právě externí firma A (sazba není totožná s Elso Service, pouze podobná).

Tabulka č.6: Časová a finanční náročnost řešení (Zdroj: Vlastní zpracování)

Změna	Řešení	Časová náročnost	Finanční náročnost
<i>Změna aplikační platformy</i>	Úprava formulářů, vytvoření nových databázových funkcí, změna designu	360 dní	1 800 000 Kč

<i>Přenesení logiky na úroveň databáze</i>	Úprava formulářů, vytvoření nových databázových funkcí	180 dní	900 000 Kč
<i>Zavedení interaktivní nápovědy</i>	Proklik do určitého místa uživatelské příručky	60 dní	300 000 Kč
<i>Prioritizace zpracování</i>	Rozšíření funkcionality pro spouštění zpracování	30 dní	150 000 Kč
<i>Zobrazení probíhajícího zpracování</i>	Nový formulář, nová databázová funkce	20 dní	100 000 Kč
<i>Kontrola práce uživatelů</i>	Zavedení speciálního softwaru	10 dní	50 000 Kč
<i>Zpracovávání údajů o cizincích</i>	Rozšíření parametrizace zpracování	20 dní	100 000 Kč
<i>Vylepšení tiskového subsystému</i>	Úprava funkcionality tiskového subsystému	10 dní	50 000 Kč
<i>Změna identifikátoru</i>	Zavedení nového identifikátoru, převodní tabulky	20 dní	100 000 Kč
<i>Kontrola uživatelů</i>	Posílení kontroly a zodpovědnosti, určení odpovědného pracovníka	-	10 000 Kč měsíčně, pro daného pracovníka
<i>Zlepšení proškolení zaměstnanců</i>	Pravidelná školení, řešeno v rámci firmy	-	-

4.2 Návrhy řešení z metody HOS

Metoda HOS, našla problémy popsané v předcházející kapitole, zde je návrh jejich řešení.

- **Zajistit dodržování bezpečnostních pravidel**

Důležité není pouze správná pravidla bezpečnosti stanovit, ale je důležité kontrolovat jejich dodržování, a to dostatečně pravidelně. Pracovníci musí mít k jejich dodržování motivaci. Musí vědět, že v případě jejich nedodržení se na to vždy přijde a budou z toho vyvozeny potřebné závěry. Jedním typem pravidel jsou ty, co se týkají technických věcí (přístupová práva, zadávání dat do systému atd.). Další typ pravidel určuje zaměstnancům, jak se mají chovat a případně s informacemi zacházet i mimo své zaměstnání.

- **Ukládat lokální data na cloud**

Ukládání dat na fyzické disky pracovních počítačů sebou může nést velké množství hrozeb, jako je ztráta dat v případě výpadku kvůli nedostatečnému zálohování, nebo také nedostatečné zabezpečení těchto zařízení. Dobrým řešením je použít na ukládání dat společný cloud případně datový server. To zajistí dobré zálohování i ochranu dat.

- **Jasně stanovit pravidla pro jednotlivé pracovníky**

Pro správný chod celé firmy, nejen jejího informačního systému, je potřeba zavést pravidla, které určují pracovní postupy. Tyto pravidla je potřeba zaměstnancům dostatečně jasně vysvětlit a zajistit jejich dodržování.

- **Zajistit kontrolu nad instalováním programů na zaměstnanecké počítače**

Toto doporučení je stejná jako u SWOT analýzy, bylo by dobré zajistit zaměstnance, který bude kontrolovat, které programy se instalovat mohou a které ne. Což zlepší celkovou bezpečnost sítě.

- **Zajistit fyzickou ochranu techniky**

Vzhledem k tomu, že firma VZP vlastní svoje servery a fyzicky se o ně stará, je důležité zajistit jejich pořádnou fyzickou ochranou. Ta by měla dostatečně zamezit případnému fyzickému napadení útočníkem nebo nějakým živlem. Je potřeba místnost, kde je tato technika umístěna chránit tak, aby se do ní nemohl dostat nikdo neoprávněný. Zároveň je dobré zvážit kamerovou ochranu, zajistit všemožná čidla a případně zavést ostrahu.

- **Zavést zodpovědnost pracovníků za data**
Odpovědnost, za data, které jsou v systému uchovávány by měla být písemně doložitelná a vždy by měl být jasný daný vlastník, který je pouze jeden.
- **Nastavit správná přístupová práva do systému**
Je potřebné zajisti správná přístupová práva pro všechny pracovníky, pracující s informačním systémem. Nejen zajistit to, aby měli přístup ke všem datům, které ke své práci potřebují, ale zároveň zrušit přístup tam, kde již není potřeba. Většina pracovníků pouze řeší to, kam přístup nemají a potřebují ho naopak tuto druhou stránku již nesdělují. Je tedy potřeba dostatečně tyto práva aktualizovat a kontrolovat.
- **Zajistit bezpečnostní povědomí uživatelů**
Tento problém má totožné řešení jako ve SWOT analýze. K potřebnému bezpečnostnímu povědomí musí firma pravidelně a zřetelně zaměstnancům říkat, co je potřeba k dosažení největší možné bezpečnosti údajů v systému dodržovat. Proto je nejlepším řešením zavést pravidelné bezpečnostní školení, které je v dnešní době i ukládáno zákonem o ochraně osobních dat. V případě nějakého bezpečnostního incidentu je potřeba dokázat, že firma pro ochranu dat udělala maximum. Na tomto školení bude zaměstnancům vysvětleno, co musí dělat pro zamezení úniku dat ze systému.
- **Zvážit nutnost přístupu na internet**
Přístup jednotlivých pracovníků na internet ze svého počítače, může znamenat hrozbu pro únik dat. Je dobré zvážit, jestli každý pracovník přístup na internet potřebuje. Zakázání internetu může vést k dobré kontrole zabezpečení, ale většina zaměstnanců rozhodně nebude s tímto krokem jen tak souhlasit, bez udání jasného a silného důvodu.
- **Zvážit nutnost připojování externích médií k počítačům**
Technická kontrola při připojování médií zaměstnanců je velmi důležitá. Tyto média mohou být nakažena virem, a proto je nutné zvážit vůbec povolení obecně tyto média připojovat. Řešením je opět využití cloudu.

4.2.1 Celkové přínosy řešení z metody HOS

Jak již bylo ukázáno v předcházející kapitole, metoda HOS zhodnotila systém jako velmi dobrý. Jak z pohledu bezpečnosti, tak i z pohledu efektivnosti. Z tohoto důvodu nebylo nalezeno velké množství kritických chyb a jde spíše o menší chyby, které vylepší celkovou celistvost systému. Většina nedostatků se týká nedostatečného specifikování bezpečnostních pravidel pro zaměstnance. Zároveň také nejsou tyto navržené postupy příliš kontrolovány, a to může i přes tak dobrý výsledek celkového systému, jeho práci zdatně ztěžovat a prodlužovat. Proto je opravdu důležité tyto pravidla přesně nastolit a striktně je dodržovat. Některé problémy se velice přibližují těm, které byly popsány i ve SWOT analýze, to potvrzuje jejich značnou důležitost. Celkově ovšem nejde jen o tu softwarovou ochranu, ale musí se dbát i na tu fyzickou. Zabezpečení serverových místností musí být co nejsilnější. Vyřešení těchto problémů ještě více podpoří celkovou bezpečnost údajů v systému.

4.2.2 Finanční a časová náročnost řešení z metody HOS

Návrhy vycházející z metody HOS jsou ve výsledku problémy, jejichž řešení se bude odvíjet v rámci firmy, a to buď v nastolení nových a přesnějších pravidel pro práci nebo ve zlepšení kontroly jejich dodržování. Proto se celkové náklady na tyto návrhy těžko odhadují stejně jako jejich časová náročnost. Zavedení nových pracovních postupů může trvat klidně i několik měsíců a vyladění systému jejich kontroly taktéž. Finanční náklady se budou týkat analýz, na kterých se následné postupy budou stavět. Tyto analýzy budou nejspíše řešeny využitím externí firmy, které si zvolí odpovídající ceníkovou částku. Popisování přesných pracovních postupů by měl dostat na starost pracovník vyššího managementu, který by měl danou problematiku zpracovat. Z toho nevyplývají žádné dodatečné náklady, vzhledem k tomu, že je to jeho náplň práce. Cloudové řešení už ovšem náklady přinese, vzhledem k velikosti firmy a daného systému se nedříve musí zjistit, jak velké úložiště bude potřeba a poté najít nejvýhodnější nabídku dodavatele.

4.3 Celkové shrnutí

Z obou analýz nám vzniklo několik možných řešení, které ve výsledku povedou ke zlepšení efektivnosti nebo bezpečnosti celého systému. Návrhy vzniklé ze SWOT analýzy jsou spíše praktické, týkající se přímo změn v rámci informačního systému jako takového. Jedná se o přidání či předělání některých z modulů, což musí být řešeno dodavatelskou firmou. Zároveň s předěláním identifikátoru či zavedení určité prioritizace potřebných procesů. V tomto případě tedy nelze řešit chyby v rámci firmy, a proto se zde nachází vyšší náklady případného opravení zjištěných chyb. Chyby byly také ale nalezeny v zavedení pravidel po zaměstnanci a zajištění bezpečnostního povědomí uživatelů. Naopak návrhy z metody HOS jsou spíše organizačního charakteru. Vzhledem k tomu, že na základě dotazníků byl systém ohodnocen velmi dobrými procenty, nebylo nalezeno příliš chyb kritického charakteru. Proto se jednotlivé návrhy týkají lepší kontroly zavedených postupů a také zlepšení již zmíněného bezpečnostního povědomí. Tyto problémy, ale rozhodně nejsou nijak méně důležité a pro fungování systému jako celku je potřeba je co nejdůkladněji řešit. Hned v několika problémech se ale obě metody shodují, což ukazuje, že jsou z určitého pohledu zásadní. Při využití těchto poznatků by se měl systém stát v celkovém obrazu lepším, a to ať už se týká efektivnosti tak i bezpečnosti.

ZÁVĚR

Ve své práci jsem popisoval informační systém Všeobecné zdravotní pojišťovny, který shromažďuje a analyzuje data svých pojištěnců. Převážně jsem se zabýval výdajovou částí, která má na celkovou práci systému velmi významný vliv. Našel jsem chyby, které systém brzdí anebo dokonce způsobují určitá bezpečnostní rizika. Následně jsem navrhl postupy, které by měly tyto problémy vyřešit a systém celkově posílit.

V první části práce jsem popsal a vysvětlil teoretický základ, o který se celá práce opírá. V průběhu jejího vypracování jsem si zároveň osvěžil znalosti týkající se problematiky informačních technologií, tyto poznatky mi následně při zpracovávání dalších částí práce pomohly.

Druhá část nejdříve popisuje samotné firmy, a to jak firmu VZP, která daný systém využívá, tak i společnost Elso Service, která systém spravuje a díky níž mám přístup k důležitým informacím. Následně je v této části popsána celková funkčnost systému společně s dvěma analýzami (SWOT a HOS), které mi pomohly nalézt problémy tohoto systému.

V poslední části práce jsou popsána přesná řešení toho, jak jednotlivé problémy vyřešit a tím zlepšit výsledný obraz celého systému. Zároveň jsou v této části tyto návrhy zhodnoceny i z časového a ekonomického hlediska, pro jejich lepší přehlednost.

Hlavním záměrem práce bylo navrhnout takové změny, které povedou k lepší efektivnosti a bezpečnosti systému. V případě zavedení řešení, které jsem v práci popsal k tomuto cíli rozhodně dojde.

Popisovaný systém je velmi obsáhlý a v rámci jedné práce jej nejde celý popsat, proto by bylo dobré na tuto práci navázat s přesnějším popisem dalších jeho částí. Systém stojí na pevných základech, a proto je dobré hledat zbylé menší nedostatky a ty řešit. Z mého pohledu funguje dobře, ale vzhledem k tomu, jak důležitá data obsahuje, musí být stále průběžně kontrolován.

SEZNAM POUŽITÉ LITERATURY

- (1) Data. *ManagmentMania* [online]. Plzeň, 2018 [cit. 2019-01-20]. Dostupné z: <https://managementmania.com/cs/data>
- (2) BÉBR, Richard a Petr DOUCEK. *Informační systémy pro podporu manažerské práce*. Praha: Professional Publishing, 2005, 223 s. : il. ISBN 80-86419-79-7.
- (3) TVRDÍKOVÁ, Milena. *Aplikace moderních informačních technologií v řízení firmy: nástroje ke zvyšování kvality informačních systémů*. Praha: Grada, 2008, 173 s. : il. ISBN 978-80-247-2728-8.
- (4) Informace. *ManagmentMania* [online]. Plzeň, 2017 [cit. 2019-03-17]. Dostupné z: <https://managementmania.com/cs/informace>
- (5) Co je proces? *Tovia* [online]. Jihlava: Tovia, 2018 [cit. 2019-01-20]. Dostupné z: https://www.tovia.cz/blog/co_je_proces
- (6) TVRDÍKOVÁ, Milena. *Zavádění a inovace informačních systémů ve firmách*. Praha: Grada Publishing, 2000, 110 s. ISBN 80-7169-703-6.
- (7) Co je to Hardware? *IT Slovník* [online]. IT-Slovník [cit. 2019-01-23]. Dostupné z: <https://it-slovník.cz/pojem/hardware>
- (8) Software. *ManagmentMania* [online]. Plzeň, 2016 [cit. 2019-01-19]. Dostupné z: <https://managementmania.com/cs/software>
- (9) BUCHALCEVOVÁ, Alena. *Metodiky budování informačních systémů*. Praha: Oeconomica, 2009, 205 s. : il., grafy, tab. ISBN 978-80-245-1540-3.
- (10) SODOMKA, Petr a Hana KLČOVÁ. *Informační systémy v podnikové praxi. 2. aktualiz. a rozš. vyd.* Brno: Computer Press, 2010, 501 s. : il., grafy, tab. ISBN 978-80-251-2878-7.
- (11) GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. *Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi. 3., aktualizované vydání*. Praha: Grada Publishing, 2015, 240 stran : ilustrace, portréty. ISBN 978-80-247-5457-4.

- (12) BASL, Josef a Roman BLAŽÍČEK. *Podnikové informační systémy: podnik v informační společnosti*. 3., aktualiz. a dopl. vyd. Praha: Grada, 2012, 323 s. : il., portréty; 25 cm. ISBN 978-80-247-4307-3.
- (13) Procesy v dodavatelském řetězci, 2012. *System Online* [online]. CCB [cit. 2019-02-02]. Dostupné z: <https://www.systemonline.cz/it-pro-logistiku/procesy-v-dodavatelskem-retezci.htm>
- (14) KOCH, Miloš a Viktor ONDRÁK. *Informační systémy a technologie*. Vyd. 3. Brno: Akademické nakladatelství CERM, 2008, 166 s. : il., grafy, tab. ISBN 978-80-214-3732-6.
- (15) Relace v databázích. *Office.lasakovi.com* [online]. 2010 [cit. 2019-01-20]. Dostupné z: <https://office.lasakovi.com/access/tabulky/relace-vazby-v-databazich-teorie/>
- (16) Normalizace relačních databází. *Programujte.com* [online]. 2008 [cit. 2019-03-17]. Dostupné z: <http://programujte.com/clanek/2008071900-normalizace-relacnich-databazi/>
- (17) Úvod do jazyka SQL. *DotNETPortal* [online]. [cit. 2019-01-20]. Dostupné z: <https://www.dotnetportal.cz/clanek/50/Uvod-do-jazyka-SQL>
- (18) Co je GDPR. *GDPR.cz* [online]. [cit. 2019-01-20]. Dostupné z: <https://www.gdpr.cz/gdpr/co-je-gdpr/>
- (19) GRASSEOVÁ, Monika, Radek DUBEC a David ŘEHÁK. *Analýza podniku v rukou manažera: 33 nejpoužívanějších metod strategického řízení*. 2. vyd. Brno: Computer Press, 2012, 325 s. : grafy, tab. + 1 CD-ROM. ISBN 978-80-265-0032-2.
- (20) KOCH, Miloš. Posouzení efektivnosti informačního systému metodou HOS. *Trendy ekonomiky a managementu* [online]. Vysoké učení technické v Brně, Fakulta podnikatelská, 2013, **VII**(16), 49-56 [cit. 2019-04-01]. ISSN 1802-8527. Dostupné z: <http://hdl.handle.net/11012/24462>

- (21) *Elso Service* [online], 2019. Brno: Elso Service Brno [cit. 2019-04-26]. Dostupné z: <https://www.elseo-systems.com/>
- (22) *VZP ČR* [online], 2019. Praha: VZP ČR [cit. 2019-04-25]. Dostupné z: <https://www.vzp.cz>
- (23) KOCH, Miloš, On-line systém pro posouzení efektivnosti informačních systémů. *On-line systém pro posouzení efektivnosti informačních systémů* [online]. Brno [cit. 2019-04-07]. Dostupné z: <https://www.zefis.cz/>

SEZNAM POUŽITÝCH OBRÁZKŮ

Obrázek č.1: Schéma informace (Zdroj: 4)	12
Obrázek č.2: Klasifikace úrovní podniku (Zdroj: 10).....	15
Obrázek č. 3: Schéma SCM (Zdroj: 13)	18
Obrázek č.4: Schéma ERP (Zdroj: 10)	19
Obrázek č.5: Normalizace (Zdroj: 16)	21
Obrázek č.6: SWOT schéma (Zdroj: 19)	24
Obrázek č.7: Ukázka výsledku metody HOS (Zdroj: 20).....	25
Obrázek č.8: Logo Elso Service (Zdroj: 21).....	26
Obrázek č.9: Logo Všeobecné zdravotní pojišťovny (Zdroj: 22).....	27
Obrázek č.10: Schéma architektury IS VZP (Zdroj: Dokumenty firmy Elso Service) ..	31
Obrázek č.11: EPC diagram procesu v rámci IS část 1 (Zdroj: Vlastní zpracování)	39
Obrázek č.12: EPC diagram procesu v rámci IS část 2 (Zdroj: Vlastní zpracování)	40
Obrázek č.13: Efektivnost systému podle HOS (Zdroj: 23).....	46
Obrázek č.14: Bezpečnost systému podle HOS (Zdroj: 23).....	47

SEZNAM POUŽITÝCH TABULEK

Tabulka č.1: Základní údaje o firmě Elso Service (Zdroj: 21)	26
Tabulka č.2: Základní údaje o VZP (Zdroj: 22)	27
Tabulka č.3: Porovnání pojišťoven (Zdroj: Vlastní zpracování)	29
Tabulka č.4: Závažnosti požadavků (Zdroj: Vlastní zpracování).....	42
Tabulka č.5: SWOT analýza IS (Zdroj: Vlastní zpracování).....	43
Tabulka č.6: Časová a finanční náročnost řešení (Zdroj: Vlastní zpracování).....	55