VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV MANAGEMENTU

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF MANAGEMENT

POSOUZENÍ INFORMAČNÍHO SYSTÉMU FIRMY A NÁVRH ZMĚN

INFORMATION SYSTEM ASSESSMENT AND PROPOSAL FOR ICT MODIFICATION

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. VLADIMÍR RYŠÁNEK
AUTHOR

VEDOUCÍ PRÁCE — doc. Ing. MILOŠ KOCH, CSc.
SUPERVISOR

BRNO 2013

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2012/2013
Ústav managementu

ZADÁNÍ DIPLOMOVÉ PRÁCE

Ryšánek Vladimír, Bc.

Řízení a ekonomika podniku (6208T097)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Posouzení informačního systému firmy a návrh změn

v anglickém jazyce:

Information System Assessment and Proposal for ICT Modification

Pokyny pro vypracování:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza problému
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

BASL, Josef a Roman BLAŽÍČEK. Podnikové informační systémy: podnik v informační společnosti. 3. aktualiz. a dopl. vyd. Praha: Grada, 2012. 323 s. ISBN 978-80-247-4307-3.
GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. Podniková informatika. 2. přeprac. a aktualiz. vyd. Praha: Grada. 2009, 496 s. ISBN 978-80-247-2615-1.
MOLNÁR, Zdeněk. Efektivnost informačních systémů. 2. rozš. vyd. Praha: Grada, 2001, 179 s. ISBN 80-247-0087-5.
SCHWALBE, Kathy. Řízení projektů v IT. Vyd. 1. Brno: Computer Press, 2007, 720 s. ISBN 978-80-251-1526-8.
SODOMKA, Petr a Hana KLČOVÁ. Informační systémy v podnikové praxi. 2. aktualiz. a rozš. vyd. Brno: Computer Press, 2010. 501 s. ISBN 978-80-251-2878-7.

Vedoucí diplomové práce: doc. Ing. Miloš Koch, CSc.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2012/2013.

L.S.

prof. Ing. Vojtěch Koráb, Dr., MBA	doc. Ing. et Ing. Stanislav Škapa, Ph.D.
Ředitel ústavu	Děkan fakulty

V Brně, dne 02.05.2013

Bibliografická citace VŠKP

RYŠÁNEK, Vladimír. *Posouzení informačního systému firmy a návrh změn.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2013. 174 s. Vedoucí diplomové práce doc. Ing. Miloš Koch, CSc..

Abstrakt

Tato diplomová práce se zaměřuje na analýzu současného stavu informačního systému za účelem odhalení jeho nedostatků a návrhu jejich odstranění. Aplikací zvolených metod zjišťuje nedostatky bezpečnostní politiky systému, na kterou se práce nadále zaměřuje. Specifikuje, jak ohodnotit aktiva a řídit rizika v podniku a také obsahuje vlastní řešení bezpečnostní politiky s využitím programu Safetica, který přispívá ke snížení pravděpodobnosti vzniku bezpečnostních incidentů v podniku.

Klíčová slova

Bezpečnostní politika, bezpečnostní incident, informační systém, ohodnocení aktiv, pravděpodobnost, řízení rizik, Safetica.

Abstract

This thesis focuses on the analysis of the current state of an information system in order to detect it´s deficiencies and to propose a motion for their elimination. Via application of selected methods, it reveals lack in the system security policy, on which this thesis further focuses. Specifies how to implement asset assessment as a part of the risk management in the company and also contains its own security policy solution using Safetica software, which helps reducing the likelihood of the company security incidents.

Keywords

Security policy, security incident, information system, asset assesment, risk management, Safetica.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce na téma „Posouzení informačního systému firmy a návrh změn“ 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 24. 05. 2013

. . . . . .
podpis

Poděkování

Rád bych touto cestou vyjádřil poděkování doc. Ing. Milošovi Kochovi, Csc. za jeho cenné rady a trpělivost při vedení mé diplomové práce. Rovněž bych chtěl poděkovat Ing. Vojtěchovi Ryšánkovi za čas a odborné rady k dané problematice. V neposlední řadě bych chtěl poděkovat Ing. Janu Pokornému a všem respondentům za vstřícnost a pomoc při získávání potřebných informací a podkladů.

V Brně dne .....

.....
(podpis autora)

Obsah

1 Úvod

Základem vědění jsou poznatky a především z nich plynoucí informace, které mohou poskytnout řadu podkladů pro další rozhodování člověka.

Informace je tedy jedna z nejnebezpečnějších zbraní na světě, respektive mj. je klíčem k úspěchu v životě, v práci, v podnikání apod. K dispozici je řada informací, které však někdy mohou narůst množstvím do stavu, kdy je obtížné jejich vyhodnocení bez automatizovaného zpracování. Cílem práce s informacemi tedy není pouze jejich nashromáždění coby shluku dat s informačním charakterem, ale především jejich efektivní uspořádání a tedy i využití. Tuto úlohu v oblasti podnikání může zajistit kvalitní informační systém.

Novodobý informační systém má určitou historii, která se v průběhu našich a světových dějin postupně vyvíjela. Existoval již v dávné minulosti, pouze si to společnost neuvědomovala. Z významového hlediska si lze pod pojmem informace představit určitá data, která mají nějakou hodnotu, kterou obohacují cílovou skupinu, pro kterou byla tato data primárně určena. Řečeno jinak, lze tato data považovat za nehmotná aktiva, obsahující vnitřní vypovídací hodnotu. Systém lze vyjádřit jako množinu nebo skupinu vzájemně uspořádaných prvků, které mají stejné vlastnosti. Pokud tedy nyní spojíme významově tato dvě slova, čili informační systém, získáme tedy logicky uspořádanou množinu nebo množiny s libovolným počtem dat se stejnými nebo podobnými vlastnostmi. Informační systém nachází uplatnění především v oblasti podnikání, kdy cíleným hledáním dat z účelově uspořádaných množin a jejich vyhodnocením obohacuje cílovou zájmovou skupinu o nové skutečnosti, o kterých před tím nevěděla nebo si jejich existenci neuvědomovala.

Aby však takový informační systém mohl úspěšně fungovat, je k tomu potřeba další prostředek, kterým jsou informační technologie. Pod tímto termínem si lze představit technické odvětví, které se zabývá fungováním počítačů, tedy jejich hmotnou částí, nebo-li hardware, který pracuje s daty, či-li s informacemi. Nemusí to tedy být pouze počítače, ale jakýkoliv elektronický přístroj, který je schopen zpracovávat nějaké informace, tedy provádět algoritmus, přijmout vstupní data, provést s nimi požadované operace a jako výsledek operací předat výstupní data k případnému dalšímu zpracování. Podíváme-li se do historie, i informační technologie měly svůj historický vývoj, který postupně přivedl na svět současnou podobu této technologie, k jejichž vrcholům můžeme řadit např. novodobé počítače se svými operačními systémy, pestrým množstvím různých programových produktů, které nabízejí uživatelům širokou škálu možností ve využití nejen v podnikání, ale i v jiných zájmových oblastech. Informační systém má vnitřní a vnější prostředí. Vnitřní prostředí obsahuje informace, tedy interní data a jejich logicky uspořádané množiny. Aby mohl in-

formační systém fungovat, musí existovat nějaký sklad a cesta ke zpřístupnění těchto dat. K vnějšímu prostředí se řadí hardware spolu s obsluhou informačního systému, dále pak i softwarové vybavení a případně i ostatní prvky, které se vyskytují v okolí informačního systému a mohou ho pozitivně nebo negativně ovlivnit.

Aby tedy podnik mohl být podnikem úspěšným, musí nejdříve efektivně pracovat s daty. To znamená především jejich komplexní vyhodnocení, nalezení relevantních vztahů mezi jednotlivými bloky informací a poskytnutí jednoznačných a srozumitelných výstupů. Oblast informačních systémů je neustále ve vývoji a situace se často mění. Všechny osoby, které jsou v kontaktu s informačními systémy, musí flexibilně reagovat na jakékoliv změny na trhu a neustále sledovat všechny trendy v této oblasti. Tyto informace jsou běžně dostupné na internetu, v novinových výtiscích, odborných časopisech a podobně. V praxi existuje řada informačních systémů, k těm známějším patří např. informační systém SAP[1]. Je tím nástrojem, který s uvedenými principy přístupu k informacím pracuje. Umožňuje sledovat informace, řídit procesy i kompletní chod podniku v komplexních, jednoduchých a jednoznačných souvislostech. Je nutné uvést, že nejen SAP, ale i ostatní informační systémy jsou v případě vhodné volby možným optimálním řešením pro dosažení úspěchu v podnikání.

Cílem této diplomové práce je zhodnocení aktuálního stavu informačního systému SAP v reálném podniku[2], nalezením jeho slabin či nedostatků využitím metod různých analýz, soustředění se na vybraný kritický nedostatek informačního systému za účelem jeho odstranění, k dosažení optimalizace podnikového informačního systému. Při řešení tohoto úkolu budou uplatněny vědomosti autora ze studia a jejich aplikace v praxi. Důležitým aspektem je reálná aplikace a praktická funkčnost navrhnutých řešení takovým způsobem, aby tato doporučení mohl posuzovaný podnik v praxi využít. Téma diplomové práce zasahuje hlavně do oboru informatiky, ale i částečně do oboru ekonomie, managementu a dovednosti kreativity.

Diplomová práce je rozdělena do dvou hlavních částí, a to teoretické a praktické. Teoretická část se zaměřuje na stručný popis informačních systémů. Dále popisuje vybrané metody, které pomohou odhalit nedostatky informačního systému. Mezi tyto metody patří měření efektivity informačního systému a posouzení osmi klíčových oblastí pomocí ZEFIS. Tato metoda spočívá ve vyplnění dotazníků vybranými respondenty, kteří pracují s posuzovaným informačním systémem SAP, a následném vyhodnocením pomocí ZEFIS, kde jsou tato data srovnána s daty získaných z ostatních podniků. Vyhodnocení těchto podkladů pomohou odhalit některé nedostatky, na které by se měl podnik zaměřit. Mezi další zvolené metody jsou zvoleny analýzy vnitřního a vnějšího prostředí, jako jsou SWOT analýza, PEST analýza a rozbor 7S faktorů. Tyto analýzy pomohou rozebrat situaci a lépe pochopit vnitřní a vnější prostředí podniku, které budou vhodné pro použití dalších analýz a lepší formulace případných závěrů. Analýza metody řízení změn, jako je například v případě úplné změny reengineering nebo částečné změny Lewinův model změn, pomohou identifikovat oblasti, způsoby a zodpovědné osoby, které se budou v dané věci změn angažovat. Teoretická část obsahuje metodiku tvorby bezpečnostní politiky, jako je ohodnocení aktiv

[1] Systémy, Aplikace a Produkty v oblasti zpracování dat

[2] Jméno na základě přání podniku nebude zveřejněno

a rizik včetně metodiky potlačení rizik. V poslední části práce je popis metody PERT, která určuje dobu trvání a ekonomické zhodnocení celého projektu.

Nedílnou součástí je i praktická část, která se postupně zaměřuje na zvolené metody vycházející z teoretické části takovým způsobem, aby byly odhaleny nedostatky námi zkoumaného informačního systému SAP. Analýza vnitřního a vnějšího prostředí pomůže odhalit nejen vazby podnikových procesů na informační systém, ale pomůže odhalit i jeho nedostatky a vazby na okolní prostředí. Vyplněním dotazníků a jejich vyhodnocení v referenční databázi ZEFIS, budou zjišťovány nedostatky informačního systému. Následnou kombinací analýzy vnitřního a vnějšího prostředí je pak stanoven jeden kritický nedostatek. Na ten se tato diplomová práce dále zaměří a pomocí vybraných metod se snaží nalézt řešení k jeho odstranění či optimalizaci.

2 Cíle práce, metody a postupy zpracování

V této části diplomové práce jsou popsány cíle, metody a postupy zpracování, které je nutné splnit za účelem optimalizace informačního systému v daném podniku, používaného nejen k hlavním procesům, ale i podpůrným procesům informačního systému jako celku.

2.1 Cíle práce

Cíle diplomové práce spočívají v komplexním ohodnocení informačního systému, a to pomocí několika analýz, zejména efektivity informačního systému a posouzení jeho osmi klíčových oblastí. Bude provedena analýza mikroprostředí a makroprostředí. U slabin informačního systému, které tyto analýzy pomohou odhalit, budou navrhnuta nápravná řešení.

Dílčím cílem první teoretické části práce je sestavení teoretických východisek potřebných pro zpracování praktické části a poté návrhu řešení v podniku z hlediska informačních systémů. Cílem druhé, praktické části, je implementace vybraných metod z kapitoly teoretických východisek a sestavení nápravných opatření, za účelem jejich odstranění. Praktická část je dělena do více částí. Každá tato část má dílčí cíl.

Dílčím cílem první praktické části je odhalení kritického nedostatku pomocí posouzení efektivity informačního systému a osmi klíčových oblastí informačního systému, propojených s analýzou vnitřního a vnějšího prostředí. Po odhalení kritického nedostatku je dílčím cílem druhé praktické části identifikace sponzorů, agentů a oblastí změn v souvislosti odstranění kritického nedostatku, který je v práci nadále analyzován. Třetím dílčím cílem je identifikace a ohodnocení aktiv, sestavení způsobu potlačení rizik a následně tak sestavení řešení bezpečnostní politiky. Další dílčí cíl je zaměřen na odhad celkové doby trvání projektu, poslední dílčí cíl v praktické části je pak zaměřen na ekonomické zhodnocení podniku z hlediska výhodnosti implementace projektu v podniku.

2.2 Metody

Jednou ze zvolených metod je analýza efektivity informačního systému a posouzení osmi klíčových oblastí HOS pomocí ZEFIS. Tato metoda zčásti spočívá ve vyplnění dotazníků respondenty a následné vyhodnocení srovnání dat v databázi tohoto programu. Dalšími metodami jsou analýza vnitřního prostředí a analýza vnějšího prostředí. Mezi metody analýzy vnitřního prostředí patří SWOT analýza, která se zaměřuje jak na vnitřní, tak i vnější prostředí pomocí analýzy příležitostí, hrozeb, silných a slabých stránek posuzovaného podniku. Další analýzou zaměřující se na vnitřní prostředí podniku je analýza 7S faktorů, která posuzuje strategie, organizace, procesy, hodnoty, kompetence, řízení a kulturu, zaměstnance. Mezi metody analýzy vnějšího prostředí patří PEST analýza, která analyzuje politické, ekonomické, sociální a technologické faktory.

Lewinův model se v praktické části zaměřuje na změny procesů v podniku. Tento model se skládá z analýzy situace, identifikace agenta změny a intervenčních oblastí, intervence a nakonec verifikace dosažených výsledků. Tato metoda byla zvolena z důvodu, že změna byla provedena pouze částečná, nikoliv úplná, k té se využívá tzv. reengineering.

Metoda bezpečnostní politiky se v diplomové práci řídí podle bezpečnostního standardu ISO/IEC 27005. Obsahem tvorby bezpečnostní politiky je ohodnocení aktiv pomocí důležitosti, integrity a finanční ztráty pro podnik. Následuje analýza hrozeb, které jsou posuzovány s aktivy na základě pravděpodobnosti vzniku hrozby a zranitelnosti aktiva. Další metodou je řízení rizik, která vychází z ohodnocení aktiv a analýzy hrozeb, kdy je sestavena matice rizik a následně sestaveny metody potlačení rizik, které v kombinaci s maticí rizik slouží k dalším postupům zpracování.

K odhadu celkové doby trvání projektu je zvolena metoda PERT, která je sestavena na základě očekávané trvání činnosti a rozptylu trvání činnosti. Ekonomické zhodnocení projektu je poslední použitou metodou složenou z přínosů a očekávané peněžní hodnoty projektu, čisté současné hodnoty a doby návratnosti investice.

2.3 Postupy zpracování

Tématem diplomové práce je analýza současného stavu informačního systému podniku, kde jsou odhaleny procesní nedostatky. Následně je vybrán jeden kritický nedostatek, na který se tato práce zaměří a navrhne jeho nápravu.

Diplomová práce je rozdělena do dvou hlavních částí, a to teoretické a praktické. Teoretická část se zaměřuje na stručný popis informačních systémů. Potom popisuje vybrané metody, které pomohou odhalit nedostatky informačního systému. Mezi tyto metody patří měření efektivity informačního systému a posouzení osmi klíčových oblastí pomocí ZEFIS a dotazníků, analýzy vnitřního a vnějšího prostředí, SWOT a PEST analýzou a rozborem 7S faktorů. Po aplikaci těchto analýz v praktické části jsou zvoleny další metody, jako je Lewinův model změn a popis metodiky ohodnocení aktiv a rizik včetně metodiky potlačení rizik. Stochastická metoda PERT popisuje metodiku určení dobu trvání celého projektu.

Praktická část je rozdělena do čtyř částí. První část identifikace problémů je provedena pomocí ZEFIS, SWOT, PEST analýz a rozboru 7S faktorů, které odhalí chybějící bezpečnostní politiku v podniku, což je stěžejní část řešení této práce. V druhé části identifikace změn je využito Lewinova modelu, kde se identifikují sponzoři, agenti a oblasti změn. Třetí fáze analýzy bezpečnostní politiky je zaměřena na identifikaci a ohodnocení aktiv, na základě kterých je provedena analýza a řízení rizik pomocí matice rizik, kde mezi nejrizikovější skupinu patří krádež aktiv, selhání hardware a komunikace. Poslední čtvrtá část návrhů změn popisuje způsoby potlačení rizik. Dále řešení bezpečnostní politiky je dle ISO/IEC 27005 navrženo aplikací vlastní režie a z části využitím podpůrného software Safetica. V závěru je metodou PERT odhadnuta délka trvání implementace nové bezpečnostní politiky v podniku a ekonomické zhodnocení.

3 Teoretická východiska práce

V této kapitole budou uvedena veškerá teoretická východiska práce, která budou z převážné části využita pro pochopení problematiky v praktické části.

3.1 Historie informačních systémů

Implementace podnikových informačních systémů v dnešní podobě, kterou velmi často symbolizují aplikace označované jako ERP, vznikla na počátku devadesátých let 20.století. Během této doby z hlediska rozvoje informačních systémů, jejich rostoucího uplatňování v podnikové praxi (a to nejen tam) a v rámci změn výrobních i nevýrobních technologií začaly být nabízeny inovované i nové výrobky a služby. (1)

Například v Detroitu se známý český podnikatel Tomáš Baťa seznámil s proudovou výrobou, jehož podstatou byl běžící pás. Zde si uvědomil, že největší hodnotu v celém výrobním procesu je čas, který lze ovlivňovat efektivním využitím strojových a lidských kapacit, přičemž peníze zde hrají roli určitého druhu neviditelného „superpásu“. Baťův úspěch v podnikání a budování jeho základů vychází právě ze sbírání informací a poznatků. Jeho úspěch tkvěl v převzetí všech nezbytných znalostí a zkušeností, jejich efektivního využití pro své vlastní podnikání. (4)

V osmdesátých letech bylo charakteristické programování vlastních úloh, kdy podnikoví analytici a programátoři vyvíjeli řešení dle požadavků a potřeb uživatelů. Na začátku devadesátých let ale požadavky trhu na straně jedné a technické možnosti dostupného hardware a software na straně druhé vedly k souvislosti s podnikovými informačními systémy ve světě k velmi významným změnám. Softwarové aplikace, které byly na začátku devadesátých let v podnicích implementovány, byly postaveny na myšlence integrace do jednoho společného řešení na principu jednotné databázové platformy, z níž čerpaly logistické, výrobní, finanční, ale i obchodní činnosti, dříve programované zvlášť. Tím začaly být postupně nahrazovány softwarové programy z předešlého období osmdesátých let, pro který byl u nás charakteristický i agendový způsob zpracování (například pro zpracování a vyhodnocení podnikových plánů, zpracování mezd apod.). (1)

Pokud nahlédneme do historie devadesátých let, pak uživatelé v podnicích sice věděli, co by mohli očekávat od aplikací informačních systémů a jejich dodavatelů, jenže to v žádném případě neznamenalo, že by došlo k určité stagnaci, protože vnitřní dynamika podnikové informační systémy dosud neopustila. (1)

V druhé polovině 20.století se začaly masivně rozvíjet technologie, zejména na západě.

Hnací sílou či motivací rychlosti vývoje stále se zdokonalujících technologií bylo, a neustále tento trend existuje, zefektivnění podnikání a dosažení tak maximálního zisku v podniku. Moderní technologie se ve 20.století přesunovala ze západu na východ a po celém světě, avšak jedna země k tomu v tomto století dodala "přidanou hodnotu ve formě zefektivnění produktivity pomocí metod (Kanban, JIT atd.). Touto zemí bylo Japonsko, jednotlivé metody se využívají dodnes po celém světě a v mnoha případech předčily některé moderní technologie. (4)

V roce 2001 došlo ke ztrátě hodnoty akcií velkého množství tzv. „dot.com" firem, avšak na počátku roku 2002 se investice do ICT začaly opět zvyšovat. Nejdříve došlo k oživení sektoru ICT v USA a poté se totéž rozšířilo do Japonska a Evropy. Tento vzestup se týkal hlavně počítačů a jejich komponent. Díky investicím do vysokorychlostního širokopásmového připojení k internetu, WiFi technologií, internetových audio a video přenosů, trh s komunikačními zařízeními v současné době roste. (1)

Aktuální změny ve společnosti jsou zřetelné v posunu od centralizace k decentralizaci v oblasti přístupu k informacím, zpracování dat, rozhodování a řízení, dopravy, zabezpečení energií a trávení volného času. Dále změna a posun ve struktuře zaměstnanosti z původní dominance zemědělství (dnes v rozvinutých zemích je již jen cca 3-8 % obyvatelstva) a následného přemístění do sektoru průmyslu (podíl v rozvinutých zemích bývá uváděn v rozmezí cca 10-20 % obyvatelstva), po přemístění pracovních sil do oblasti služeb, které zahrnují nové profese a využití IT. Posun od technologických aspektů produkčního cyklu ke společensko - přírodním vede ke zlepšení pracovních podmínek a ergonomie pracovišť, ke zlepšení vztahu výrobců k životnímu prostředí formou využívaných technologií integrovaných již do návrhu nových výrobků, zohledňujících i fázi likvidace výrobku po ukončení doby jeho životnosti. Pro každý podnik z hlediska informačního systému je důležité plnit individuálně požadavky každého jednotlivého zákazníka („serve a single customer") od prvního obchodního kontaktu až po prodej výrobku či služby, reagovat prakticky v nulovém čase („act in zero time") na požadavky zákazníka a na příležitosti trhu k nabízení nových produktů, a to trvale s využitím simultánní celopodnikové spolupráce. (1)

3.2 Informační systém a informační technologie

Informační systém (IS) je množina nebo soubor lidí, technických prostředků (hardware) a metod (software), zajišťující sběr, přenos, zpracování, uchování dat, s cílem prezentace informací pro potřeby uživatelů pracujících v systémech řízení. Informační technologie (IT) jsou určité nástroje, metody a znalosti ke zpracování dat. Někdy se tento pojem označuje jako ICT, což je v podstatě to samé, ale rozšířené o komunikaci z hlediska informačních technologií. (2)

3.2.1 Podnikové zdroje informačních systémů

Plánování podnikových zdrojů je metoda efektivního plánování a řízení všech dostupných podnikových zdrojů ve výrobním nebo distribučním podniku zaměřeném na služby.

Tyto zdroje jsou nebytně důležité k přijetí a realizaci objednávky zákazníka včetně následného dodání a fakturace. (1)

Pokud budeme hovořit o implementaci nejlepších praktik, tak při zlepšování podnikových procesů zde hrají klíčovou roli moderní informační systémy. Podnik ale musí nejdříve od základů změnit způsob své organizace a řízení, jedná se o transformaci z funkčně orientované organizace na procesně řízený podnik, tedy zavedení procesního managementu. Procesní organizace by pak měla sestavit a řídit práci tak, aby se výsledek jevil jako ucelený proces, který je dekomponován na jednotlivé, vzájemně logicky provázané podprocesy. (4)

ERP[1] v užším vymezení zahrnuje integraci softwarových nástrojů v podnicích a funkčnosti softwarových nástrojů, jako je výroba (včetně dat o výrobku), logistika, finance a lidské zdroje. V širším slova smyslu pak rozšířené („extended“) ERP zahrnuje další aplikace, jako jsou manažerské nadstavby typu BI („Business Intelligence“) a aplikace podporující vazby podniku na jeho okolí, například řízení dodavatelských řetězců v podobě SCM („Supply Chain Management“), a řízení vztahu se zákazníky formou aplikací označovaných jako CRM („Customer Relationship Management“). Nedílnou součástí integrovaných celopodnikových řešení typu ERP se dále stávají komponenty pro realizaci elektronického obchodu - B2B („Business to Business“), B2C („Business to Customer“) a zásobování („e-procurement“). (1)

Nedílnou součástí podnikových IS, kterou je nezbytné si zde uvést, je finanční funkcionalita. V IS bývá aplikován princip integrovaného zpracování všech dat z dokladů, čímž je dosahováno synchronní aktualizace informací nejen ve finančním účetnictví, ale i v ostatních modulech IS. Nedílnou součástí finanční funkcionality podnikových IS se stala na počátku tohoto desetiletí i integrace a harmonizace ve vztahu k legislativě EU a integrace eura. Účetnictví by dále mělo splňovat obecně uznávané účetní postupy *Souboru obecně přijatých účetních zásad* - například GAAP[2] a mělo by být aplikováno na lokální podmínky i v době měnících se legislativních opatření. U ekonomických IS pro malé a střední podniky se obvykle ještě v nabídce vedle funkcionality týkající se logistiky objevují moduly, jako jsou knihy jízd, propojení na MS Office, propojení na internetový obchod atd. (1)

CRM koncepce je založena na úzké provázanosti IS a řízení externích procesů, jejichž spoluvlastníkem jsou zákazníci podniku. **SCM** koncepce je založena na úzké provázanosti IS a řízení externích procesů, jejichž spoluvlastníkem jsou dodavatelé podniku nebo odběratelé podniku. (4)

Při pohledu na nabídku současných podnikových IS se lze setkat obecně se dvěma typy aplikací rozlišovaných podle typu jejich specializace na straně jedné a komplexnosti na straně druhé:

- *All-in-One* - tyto aplikace pokrývají všechny klíčové podnikové procesy, respektive jejich většinu. Na jedné straně je pro ně charakteristická vysoká úroveň integrace, na druhé straně mohou nabízet nižší detailní funkcionalitu.

- *Best-of-Breed* - tyto aplikace se zaměřují na pokrytí vybraných procesů a na jejich

[1] Enterprise Resource Planning - plánování podnikových zdrojů
[2] Generally Accepted Accounting Principles

specializaci. Je pro ně charakteristická vysoká detailní funkcionalita spojená naopak se složitější integrací. (1)

Kromě toho je snaha dodavatelů o nabídku určitých jednodušších odlehčených „lite“ verzí řešení aplikací pro podnikové IS. Dále je patrné i postupné rozšiřování nasazování nástrojů podporujících podnikové IS i v nepodnikové sféře, kam patří například veřejná správa, zdravotnictví nebo školství. (1)

Veškeré podnikové procesy by měly být dále měřeny a kontrolovány. Pokud dojde k odhalení rozdílů mezi klíčovými výkonnostními indikátory KPI[3], určenými na strategické úrovni a skutečnými hodnotami KPI, pak musí dojít ke zlepšování procesů. Může však dojít k situaci, kdy dojde k zásadním proměnám okolí nebo vnitřních podmínek podniku, taková situace je vyřešena na strategické úrovni. Klíčem k úspěchu řízení podniku je její procesní orientace, kde by se podnik měl zaměřit a respektovat nutnost průběžných inovací vnitropodnikových procesů. Takto orientovaná společnost má výhodu v tom, že může flexibilně reagovat na okolní změny a získává tak širokou adaptabilitu. Jako příklad si lze uvést nově příchozího dodavatele nebo zákazníka, novou tržní příležitost, akvizici jiného podnikatelského subjektu apod. Procesně orientovaný podnik je schopen odhalit a analyzovat své vlastní nejužší místo, což umožní efektivně plnit nejen krátkodobé potřeby, ale i dlouhodobě úspěšně konkurovat na trhu. (4)

3.2.2 Informační strategie

Neexistence informačních strategií v podniku je hlavní příčinou neefektivních výdajů na IS/IT. Informační strategie obecně spočívá v soustavě cílů a ve způsobech jejich dosažení. Tvorba informační strategie v podniku by měla být vedena trvalým dialogem mezi obecným managementem podniku a odborníky informatiky. Úroveň informační infrastruktury by měla trvale mírně předbíhat úroveň IS/IT podniku, což je zázemí pro trvalý rozvoj IS/IT. Proces formulace informační strategie by se měl ptát na otázky u podnikatelské strategie PROČ? U informačního systému CO?, u informační technologie JAK? a u informačního managementu KDO?, KDY?, ZA KOLIK?. (2)

3.2.2.1 Monopol

Aplikace pro IS/IT jsou stanoveny jediným útvarem pro všechny uživatele. Výhodou této strategie je, že výdaje jsou velmi dobře kontrolovatelné. Nevýhodou jsou situace, kdy uživatelé nejsou příliš spokojeni se zvolenými aplikacemi a nemusí zohledňovat potřeby konkurenceschopnosti společnosti. Tato strategie je typická u bank, pojišťoven apod. (2)

3.2.2.2 Centrální plánování

Strategie je plně integrována s podnikatelskou strategií a je řízena útvarem pro IS na vrcholové úrovni. Je zde vyžadována přímá angažovanost vrcholového managementu. (2)

[3]Key Performance Indicators

3.2.2.3 Vedoucí role

Využívá nejmodernější technologie, ale tím čerpá obrovské náklady. Uskutečnění této strategie je často velmi rizikové a bez podpory vrcholového managementu by neměla být vůbec aplikována. (2)

3.2.2.4 Volný trh

Zde hrají důležitou roli uživatelé IS/IT, u kterých se předpokládá, že jej nejlépe znají. Útvar pro IS/IT musí čelit konkurenci externích podniků a má nízkou podporu vrcholového managementu, což může vést k plýtvání podnikových zdrojů a nerovnoměrnosti vývoji IS/IT. (2)

3.2.2.5 Omezené zdroje

Jedná se o způsob řízení IS/IT, kdy jsou předem stanovené výdaje finančními manažery. Posuzuje se hlavně jejich návratnost. (2)

3.2.2.6 Nezbytné zlo

IT je aplikovaná pouze tam, kde to vyžadují předpisy nebo kde neexistuje jiná alternativa řešení problémů, k tomu navíc aplikace musí přesvědčit management vysokou návratností. Tohle může vést ke ztrátě motivace kvalifikovaných pracovníků a odchodu z podniku. (2)

Čím více se musí podnik spoléhat na IS/IT jako na strategický nástroj, musí být v podniku nějaká osoba, která bude za fungování IS/IT zodpovědná. Tato osoba se nazývá CIO[4], v ČR je to ředitel pro informační systémy nebo tzv. IT manažer. (2)

3.2.3 Druhy informačních systémů

V následující podkapitole bude uvedeno několik druhů informačních systémů, hlavně ty největší, jako je například SAP a stručně budou popsány. Nejdříve je třeba rozlišit **holisticko-procesní klasifikaci**:

- *ERP* - Jádro, zaměřené na řízení interních podnikových procesů.
- *CRM* - Systém obsluhující procesy směřované k zákazníkům.
- *SCM* - Systém řídící dodavatelský řetězec, jehož integrální součástí bývá APS systém sloužící k pokročilému plánování a rozvrhování výroby.
- *MIS* - Manažerský informační systém, který sbírá data z ERP, CRM a APS/SCM systému (a samozřejmě také z externích zdrojů) a na jejich základě poskytuje informace pro rozhodovací proces podnikového managementu. (4)

[4]Chief Information Officer

3.2.3.1 Systémy, aplikace a produkty v oblasti zpracování dat

SAP je největším světovým dodavatelem aplikačního software pro podniky a organizace všech velikostí. Celkově více než 76000 zákazníků ve 120 zemích světa využívá SAP software. Na českém trhu působí společnost SAP od roku 1992 a dosud získala více než 750 českých zákazníků z podnikové sféry, finančních institucí a organizací veřejné správy. Mezi zákazníky patří nejen menší a střední podniky, ale i velké společnosti a podniky. Tento informační systém je stabilní, dynamicky se rozvíjející platforma pro řízení podnikových procesů. Je celosvětově osvědčený v nejrůznějších oblastech lidské činnosti od výroby, přes poskytování služeb, až po veřejnou správu. (5)

V rámci projektů bylo dosaženo významných synergických efektů a optimalizace procesů. Samotná společnost SAP, která software vyvinula, byla založena v Německu již v roce 1972 bývalými zaměstnanci IBM. Její nejznámější produkt je SAP R/3. Jeho novější verze se jmenuje mySAP. Produkt SAP R/3 se skládá z modulů finančního účetnictví, kontrolingu, evidence majetku, plánování dlouhodobých projektů, řízení oběhu dokumentů, specifického řešení různých odvětví, řízení lidských zdrojů, údržby, skladového hospodářství a logistiky, managementu kvality, plánování výroby a podpory prodeje. Technologie SAP R/3 spočívá ve využívání třívrstvého modelu. První vrstva je prezentační, kdy uživatel komunikuje s klientem, druhá je aplikační a třetí databázová. Funkčnost systému je programována vlastním jazykem ABAP[5]. (1)

3.2.3.2 Microsoft Dynamics

Tento produkt Microsoftu vstoupil na trh v roce 2002 odkoupením dánského systému Navision. Později zahrnul do portfolia Microsoft Business Solution, tedy podnikové řešení. Později stále rozšiřoval produktové portfolium až se z něho začal stávat velmi silný hráč. Tak vznikl Microsoft Dynamics, který dodnes velmi silně ovlivňuje postavení ERP systémů na trhu. Hlavní konkurenční výhoda spočívá ve variabilitě možných postupů oproti ostatním konkurentům na trhu. Jen pro zajímavost, v letech 2003-2004 Microsoft vyjednával neúspěšně se společností SAP o odkoupení softwarového produktu. (4)

3.2.3.3 Oracle

ERP systém Oracle DMBS, neboli *Oracle database management system*, v překladu *systém řízení dat*, je moderní databázový systém, pyšnící se velmi pokročilými možnostmi zpracování dat, vysokým výkonem a snadnou přenositelností. Oracle business intelligence je komplexní a kompletní řešení pro všechny potřeby analýz, a to jak základních (reportování a „ad hoc“[6] dotazování vyskytující se například u SQL databází), tak i pokročilých (OLAP[7] a Data Mining[8]). Toto řešení nabízí snadnou tvorbu analýz nad relačně a multidimenzionálně uloženými daty a jejich prezentování v rámci podniku nebo mimo něj.

[5]Advanced Business Application Programming

[6]Z latinského překladu „pro tento účel“

[7]Online Analytical Processing - technologie uložení dat v databázi

[8]Získávání složitých skrytých a užitečných informací z dat.

Umožňuje i vývoj vlastních analytických aplikací, správu metadat, návrh a monitoring datového úložiště. (17)

3.2.4 Služby z hlediska informačních systémů a technologií

K vybraným dodatečným službám z hlediska informačních systémů, které se v praxi mohou objevit je outsourcing a service level agreement (SLA).

3.2.4.1 Outsourcing

Pod pojmem outsourcing si lze představit využívání externích(cizích) zdrojů pro jakoukoliv činnost, která je nebo byla doposud prováděna vlastními podnikovými zdroji. Je to tedy služba zajišťovaná jinou společností na náklady objednatele. Takovým příkladem může být např. vedení účetnictví externím podnikem pro jejího objednatele, čili zákazníka. Výhodou této služby je, že podnik může outsourcovat některé vedlejší procesy a může se tak soustředit na hlavní procesy ve svém podniku a tím významně např. zvýšit efektivitu v podniku. (2)

3.2.4.2 Service Level Agreement

SLA je jedna z komponent součástí služeb, která se v poslední době často diskutuje. Je to jedna z velmi důležitých součástí efektivního řízení SSC[9] . Nemůže být jednoduše kopírovaná z jiného podniku, ale musí být vytvořena na míru dle požadavků podniku. Obecně to je smluvní vztah mezi poskytovatelem služeb a zákazníkem, v tomto případě tedy podnikem, který této služby informačního systému využívá ke své činnosti. Využití SLA je nezávislé bez ohledu na to, je-li podnik SSC organizovaným podnikem jako samostatná právní jednotka nebo není takto organizován. V obou případech je SLA stále vyžadována na základě podnikatelských potřeb, specifikuje rozsah služeb, úroveň služeb a stanovení cen. Obsahuje následující základní složky:

- *Rozsah poskytovaných služeb* - závazný seznam poskytovaných služeb.
- *Popis zákaznických služeb* - osnova, jak se poskytovatel služeb bude starat o zákazníka.
- *Informace o nákladech* - stanovení cen za poskytnuté služby.
- *Externí benchmarky* - srovnávání úrovně a cen poskytovaných služeb oproti jiným podnikům.
- *Výkonnostní úroveň závazků* - splněné závazky od poskytovatelů na základě měření klíčových ukazatelů výkonnosti.

[9]Shared Service Center - centrum sdílených služeb

- *Zákaznické závazky* - osnova všech zákaznických požadavků, které poskytovatel musí závazně splnit.
- *Zlepšení procesů* - zodpovědnost z hlediska iniciativy zlepšení procesů.
- *Řešení problémů* - soupis, jak budou řešeny problémy a nespokojenost mezi poskytovatelem služby a zákazníkem.
- *Smluvní podmínky* - obsahující délku trvání smlouvy a možnosti rozvázání smluvního vztahu.

Samozřejmě SLA může obsahovat více složek. Podstatné však je, že poskytovatel služeb je zodpovědný za smluvně podložené procesy v podniku a pokud je nedodrží, hrozí mu finanční postihy. (22)

3.3 Řízení procesů změn v informačním systému

Cílem řízení změn je usnadnění a urychlení průběhu změny, aby předem zvolená strategie byla úspěšně a efektivně implementována. Zde je třeba zdůraznit důležitost lidského faktoru a i přes svou důležitost nepřeceňovat vliv software či hardware, kdy přílišným soustředěním se na tyto dva faktory může dojít k neúspěchu zavádění a využití IT projektů v praxi. Mnohem důležitější je, zda chceme měnit celý proces od začátku nebo stávající proces pouze kontinuálně vylepšovat dále uvedenými metodami. (4)

3.3.1 Business Process Reengineering

BPR je zcela jiným přístupem oproti průběžnému zlepšování procesů. Ve své podstatě je předpokladem k řešení zcela nevyhovující, nefunkční, špatný podnikový proces, který je třeba úplně změnit od počátku. Tento přístup umožňuje pohled na danou věc z úplně jiného hlediska. Soustředí se na úplně nový proces a umožňuje odpoutat se od současného stavu procesu. Reengineeringový přístup má několik kroků, které začínají definicí rozsahu projektu, analýzou potřeb a možností, vytvořením soustavy procesů, naplánováním přechodu a nakonec implementací. Pokud porovnáme metodu průběžného zlepšování a reengineeringu, můžeme první metodu označit zlepšením a druhou pak inovací. (3)

3.3.1.1 Metodika Hammera a Champyho

Tato metodika se zabývá fundamentálním přemýšlením a radikální rekonstrukcí strategicky kritických podnikových procesů. Jako hlavní problémy podniků vidí nedostatečný management a nejasné cíle. Jejich zlepšení jsou hlavními faktory úspěchu reengineeringu. Okrajově je pak uvažován možný odpor zaměstnanců jako hlavní překážka zavedení nového systému podnikových procesů. (3)

3.3.1.2 Metodika T. Davenporta

Kritickým faktorem reengineeringu podnikových procesů jsou podle T.Davenporta informační technologie pro svůj potenciál inovace. Patří sem záležitosti organizační a personální, jinými slovy chování. Podniková kultura je zde považována za důležité omezení. Z hlediska řízení změny se tato metodika vztahuje k tradičnímu funkčně-liniovému řízení, kam patří plánování, přikazování, sledování, rozhodování a komunikace. (3)

3.3.1.3 Metodika Manganelliho a Kleina

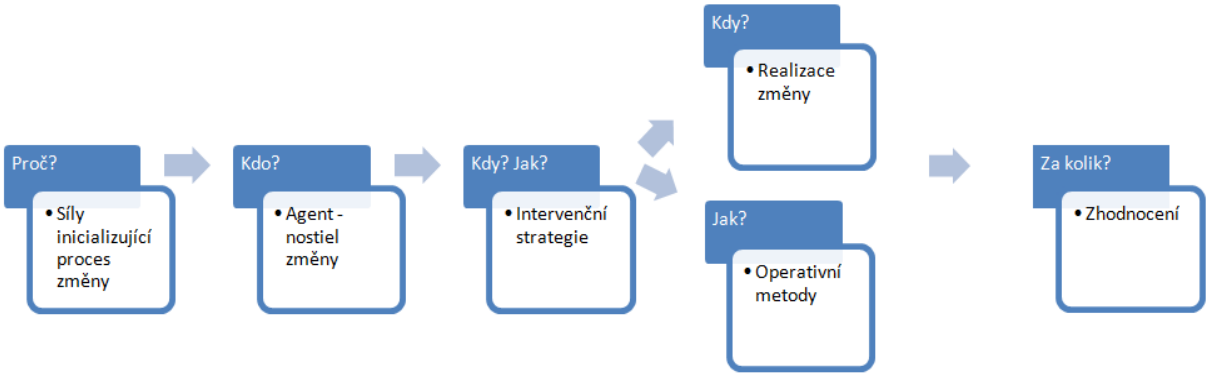
Metodika doporučuje zaměření se na ty procesy, které souvisí se strategickými cíly podniku a s požadavky jejich zákazníků. Důležitou roli zde hraje součást podnikového procesu – vývoj produktu, tedy znalostní proces. Mezi hlavní překážky úspěchu jsou řazeny dopady na podnik jako celek, čas, náklady a rizika. Reengineering musí být úspěšný, ne evoluční. (3)

3.3.1.4 Metoda Kodak

Metoda byla vyvinuta za účelem její aplikace při řešení typických problémů obrovských nadnárodních podniků po celém světě, především za účelem reengineeringu sebe sama. U této metody je reengineering podnikových procesů značně ovlivněn přístupem Hammera a Champyho. (3)

3.3.2 Lewinův model

Důležité je správné načasování a vzájemná posloupnost jednotlivých činností. Uvedené jednotlivé fáze procesu řízené změny v podniku jsou v podstatě jednotlivými kroky Lewinova modelu (obrázek 3.1). (12)



Obrázek 3.1: Lewinův model řízené změny

3.3.2.1 Analýza situace

Prvním krokem v procesu řízené změny musí být rozhodnutí, zda je nutné provést plánovanou změnu či nikoliv. Toto rozhodnutí bude závislé na výsledku analýzy sledovaného podniku, například pomocí STEP analýzy, Porterova modelu, SWOT analýzy a dalších. Výsledkem pak bude, zda je současný stav vyhovující, uspokojivý nebo nevyhovující. Dále je vhodné provést analýzu rizik, tedy analýzu sil, které působí pro a proti plánované změně. (12)

3.3.2.2 Identifikace agenta změny

Jak je uvedeno na obrázku 3.2, agentem změny může být jednotlivec (interní, externí) nebo skupina zaměstnanců, kteří budou nositeli celého procesu změny v podniku. Agent změny je podporován sponzorem změny, což obvykle bývá majitel, spoluvlastník apod. Bude nás pak zajímat flexibilita zaměstnanců, ochota akceptovat proces změny, stupeň očekávaného rizika a stupeň nespokojenosti se současným stavem. (12)

Obrázek 3.2: Čtyři základní kategorie pracovníků v podniku

3.3.2.3 Identifikace intervenčních oblastí

Identifikace oblastí, ve kterých bude provedena intervence, zásahy budou směrovat do oblastí lidských zdrojů a jejich řízení, organizační struktury podniku, technologie podniku, komunikačních a organizačních toků a procesů v podniku. (12)

3.3.2.4 Intervence (vlastní změna)

Modelem plánované změny obvykle chápeme projekt, který je tvořen souborem na sebe navazujících činností. Implementaci plánované změny v podniku lze rozložit na tři nava-

zující fáze, a to na rozmrazení, vlastní změnu a zamrazení. Ve fázi rozmrazení je nezbytné připravit podmínky pro provedení změny. Druhá etapa představuje vlastní provedení změny s cílem dosažení požadovaných parametrů podnikem. Poslední fází je zamrazení, tedy zakonzervování žádoucího stavu, aby nedocházelo k tendenci vrátit se k původnímu stavu. (12)

3.3.2.5 Verifikace dosažených výsledků

Obsahem závěrečné fáze je zhodnocení dosažených výsledků při provádění řízené změny v podniku. (12)

3.3.3 Model plovoucího ledovce

Tato metoda je z pohledu na změnu komplexnější. Podstatou je předpoklad, že převážná část manažerů pohlíží na řízení změny technokraticky. Metoda se opírá o trojrozměrnost projektu, tzv. **trojimperativ**, který je tvořen náklady, časovým harmonogramem a jeho obsahem. Pokud se ale tato změna řídí pouze tímto trojimperativem, většinou projekt nebývá úspěšný. Řešení projektu se označuje špičkou ledovce, kterou je vidět nad hladinou, pod hladinou pak existují další dvě dimenze řízení změn a zavádění. První dimenze se nazývá řízení vnímání a mínění, druhá dimenze se nazývá řízení síly a zájmů. (4)

Podstatou strategie změny je vycházení z aktuální situace, ve které se daný podnik nachází. Potom může být tato strategie pojata buď jako revoluční, skoková transformace nebo jako evoluční, inkrementální vylepšování. Provedení změny je ovlivněno čtyřmi skupinami lidí.

První z nich jsou *příznivci* vyznačující se pozitivním obecným postojem ke změně, druhou skupinou pak *oponenti*, kteří mají jednoznačný negativní obecný postoj ke změně. Další skupinou jsou *oportunisté*, kteří sice zaujímají negativní obecný postoj ke změně, ale navenek tuto změnu podporují. Poslední skupinou jsou *potencionální příznivci*, kteří změnu pozitivně hodnotí navenek, ale uvnitř nejsou přesvědčeni o prospěšnosti plánované změny. (4)

3.4 Analýza vnitřního a vnějšího prostředí

Pro analýzu vnitřního a vnějšího prostředí si uvedeme tři základní nástroje, a to rozbor 7S faktorů, který představuje obecnou analýzu vnitřního prostředí podniku. Rozbor je postavena na předpokladu, že úspěšný podnik musí mít v souladu určité elementy, faktory 7S. Druhým nástrojem je SWOT analýza, která slouží jak pro analýzu vnějšího a zároveň vnitřního prostředí. Třetím nástrojem je PEST analýza, která zkoumá pouze vnější prostředí. (4)

3.4.1 Rozbor 7S faktorů

Mezi hlavní faktory úspěchu patří struktura podniku, strategie, spolupracovníci v podniku, jejich dovednosti, styl řízeného podniku, systémy (postupy v podniku) a sdílené hodnoty podniku, jinými slovy kultura podniku. (12)

Tento manažerský model byl vytvořen Robertem H. Watermanem, Jr. a Tomem Petersonem v podniku McKinsey v roce 1980. Analýza neboli rozbor 7S v podniku McKinsey (anglicky McKinsey 7S Framework) je určena k analýze vnitřního prostředí podniku. V podstatě monitoruje veškeré změny uvnitř podniku a jeho současnou situaci. Princip tkví v předpokladu sladění všech částí 7S modelu. Model tedy může napomoci identifikovat potřeby změn vedoucích ke zlepšení situace v podniku. Analýzu je vhodné použít pro obecnou analýzu. Je založena na předpokladu, že úspěšný podnik musí mít v souladu určité elementy. Tato analýza obsahuje 7 elementů, které jsou rozděleny na **tvrdé** a **měkké**. (16)

Mezi **tvrdé elementy** řadíme:

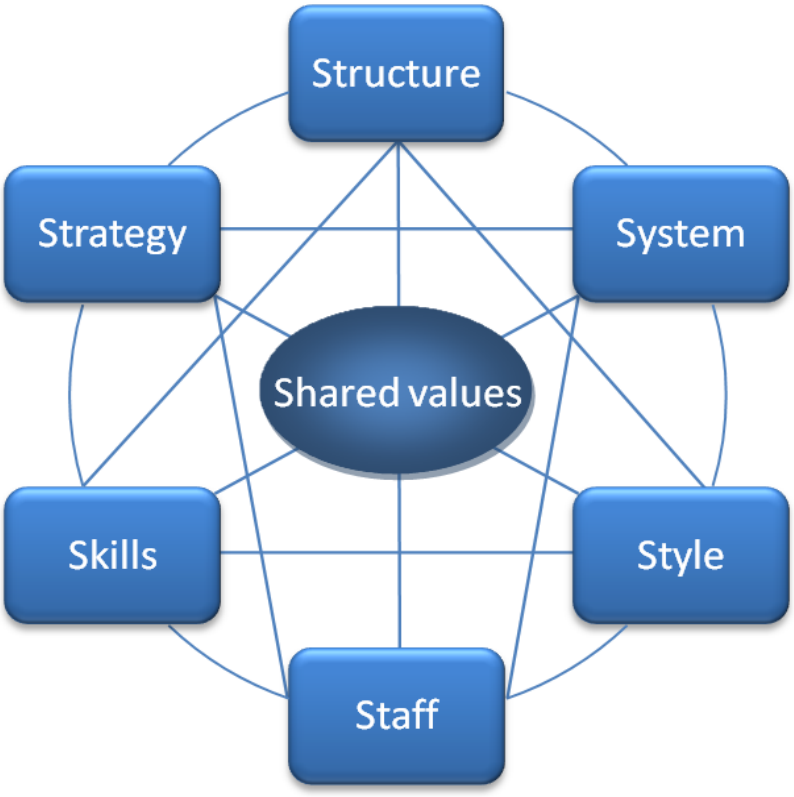
- **Strategy**(strategie) - promyšlený plán, jak udržet a vybudovat výhodu nad konkurencí.
- **Structure** (organizace) - jak je organizace členěná a kdo se komu v podniku zodpovídá.
- **Systems** (procesy) - denní aktivity a procesy, které zaměstnanci v podniku provádí, aby odvedli dobrou práci.

Mezi **měkké elementy** patří:

- **Shared values** (hodnoty) - nazývané *nadřazenými cíly*, které jsou jádrem hodnot v celém podniku evidované jako korporátní kultura a obecná pracovní etika.
- **Skills** (kompetence) - aktuální schopnosti a kompetence pracujících zaměstnanců v podniku.
- **Style** (řízení a kultura) - způsob řízení zaměstnanců, styl přijatého vedení a podniková kultura.
- **Staff** (zaměstnanci) - zaměstnanci a jejich obecné schopnosti.

Tato analýza se používá především pro:

- Zlepšení výkonnosti podniku.
- Prozkoumání možných dopadů budoucích změn ve společnosti.
- Srovnání oddělení a procesů během fúze nebo akvizice.
- Určení nejlepšího způsobu implementace navrhnuté strategie. (16)



Obrázek 3.3: McKinseyho 7S Model

3.4.2 SWOT analýza

Analýza SWOT odhaluje na základě strategického auditu silné (Strengths - S) a slabé stránky (Weaknesses - W), příležitosti (Opportunities - O) a hrozby (Threats - T). Audit nabízí různorodé množství dat odlišného významu a spolehlivosti. Analýza SWOT tato data vyhodnocuje a zdůrazňuje hlavní položky vyplývající z interního i externího auditu. V zájmu větší působivosti se jedná o menší počet položek, které poukazují na to, kam by měl podnik upřít svou pozornost. (7)

Cílem SWOT analýzy je identifikovat, do jaké míry je relevantní současná strategie podniku a její specifická silná a slabá místa, která jsou schopná se vyrovnat se změnami, které nastávají v určitém prostředí. Doporučuje se začít OT analýzou **makroprostředí** (obsahuje faktory politicko-právní, ekonomické, sociálně-kulturní, technologické) a **mikroprostředí** (zákazníci, dodavatelé, odběratelé, konkurence, veřejnost). Po důkladně provedené OT analýze následuje analýza SW, která se týká vnitřního prostředí podniku (cíle, systémy, procedury, podnikové zdroje, materiální prostředí, podniková kultura, mezilidské vztahy, organizační struktura, kvalita managementu a podobně). (8)

Úkolem managementu podniku je najít příležitosti a hrozby ovlivňující daný podnik, které se zapíšou do tabulky 3.1. Totéž bude provedeno pro příležitosti podniku, které

Silné stránky *strengths* zde se zaznamenávají ty skutečnosti, které přinášejí výhody nejen zákazníkům, ale i podniku	**Slabé stránky** *weaknesses* zde se zaznamenávají ty skutečnosti, které podniku přitěžují, nebo ty, ve kterých si ostatní podniky vedou lépe
Příležitosti *opportunities* zde se zaznamenávají skutečnosti, které mohou zvýšit poptávku nebo mohou lépe uspokojit zákazníky a přinést podniku úspěch	**Hrozby** *threats* zde se zaznamenávají skutečnosti, jako jsou trendy, události, které mohou snížit poptávku nebo zapříčinit nespokojenost zákazníků

Tabulka 3.1: SWOT analýza

se týkají vnitřního prostředí. Vyplněním tabulky je možné získat celkový přehled všech příležitostí a hrozeb, silných a slabých stránek, což může být později využito k tvorbě strategií, které budou tvořeny za účelem eliminace hrozeb a slabých stránek a maximální využití příležitostí a silných stránek.

OT-SW	**Silné stránky**	**Slabé stránky**
Příležitosti	Maxi - Maxi	Maxi - Mini
Hrozby	Mini - Maxi	Mini - Mini

Tabulka 3.2: Tvorba podnikových strategií vycházející ze SWOT analýzy

Na vypracovanou SWOT analýzu je možné vytvořit strategie, které maximalizují silné stránky a příležitosti a minimalizují slabé stránky a hrozby, tak jak je uvedeno v tabulce 3.2. Cílem je využití všech informací ze SWOT analýzy k vytvoření vhodných strategií, pomocí kombinací SO (Maxi-Maxi), WO (Maxi-Mini), ST (Mini-Maxi) a WT (Mini-Mini). Tyto strategie pak mohou být velmi užitečné pro daný podnik a odhalit negativní skutečnosti, které nejsou na první pohled patrné.

3.4.3 PEST analýza

Analýza prostředí je důležitá pro poznání externího okolí, ve kterém podnik působí, dále pro identifikaci změn a trendů, které se dějí v okolí podniku a mohou mít na něj vliv, dále pak stanovení toho, jak bude podnik na vlivy těchto změn a trendů reagovat. PEST analýza představuje analýzu **P**olitických, **E**konomických, **S**ociálních, **T**echnologických faktorů prostředí, které mohou ovlivnit podnikání a rozvoj podniku. Do sociálního prostředí se zahrnuje i demografické a kulturní prostředí. (9)

Vysoké ceny bydlení, dostupné prostředky pro plánování rodičovství a sociální změny

Faktory			
Politické	**Ekonomické**	**Sociální**	**Technologické**
Politická stabilita	Daňové zatížení	Přístup k práci a volnému času	Rychlost zastarávání
Pracovní právo	Vývoj cen energií	Úroveň vzdělávání	Změny technologie
Regulace v oblasti zahraničního obchodu	Průměrná mzda	Mobilita	Nové objevy
Daňová politika	Nezaměstnanost	Změny životního cyklu	Celkový stav technologie
Ochrana spotřebitele	Inflace	Demografický vývoj populace	Vládní podpora

Tabulka 3.3: Příklady faktorů sledovaných v rámci PEST analýzy

v počtu žen, které se chtějí věnovat kariéře, znamenají, že mnoho lidí hledá vlastní bydlení později a má méně dětí. Společný vliv těchto makroekonomických prvků tento svět během příštích desetiletí významně změní, vzhledem ke stárnutí populace, menšímu počtu dětí a růstu počtu závislých osob. V současnosti se trhy mění, protože mladí lidé často bydlí u rodičů až do třiceti let a mnoho lidí se rozhodne pro partnerství bez dětí, ale zato s dvojím příjmem, a to raději takto, než by čelili sociálním a ekonomickým nákladům rodičovství. Podobným způsobem bude analyzováno makroprostředí posuzovaného informačního systému. (7)

3.5 Deterministické a stochastické metody

Pokud má být pochopena problematika stochastické metody PERT, které bude v této práci využito, měla by nejdříve být popsána metoda CPM, která má podobný, ale jednodušší princip řešení, přičemž stochastická metoda PERT z ní nepřímo vychází a zobecňuje ji. Obě metody však vycházejí ze síťového hranově ohodnoceného grafu. (11)

3.5.1 Deterministická metoda CPM

Tato metoda vznikla v roce 1957 v podniku Du Pont de Nemours & Co., kde pomohla zkrátit celý projekt až o dva měsíce. Metoda CPM[10] je deterministická metoda, která vychází z předpokladu, že doby trvání jednotlivých dílčích činností je možno přesně určit, přičemž nebere v úvahu náhodné vlivy. Umožňuje stanovit (s využitím sestrojeného síťového grafu) nejkratší možnou dobu trvání projektu, stanovit kritické činnosti i kritickou cestu projektu, určit rozmístění a velikost časových rezerv. Při řešení problému pomocí metody CPM je pro všechny dílčí činnosti nezbytné určit tyto čtyři časové údaje:

[10] z anglického Critical Path Metod

- $NMZ_{i,j}$ - *nejdříve možný začátek činností* počínajících v uzlu i. Žádná z dílčích činností s počátkem u_i nemůže začít dříve, než budou ukončeny činnosti, které v tomto uzlu končí. (Uvedený údaj je dále označován symbolem $t_i^{(0)}$).

- $NMK_{i,j}$ - *nejdříve možný konec činnosti* počínající v u_i a končící v u_j. Tato činnost je v síťovém grafu zobrazena hranou h_{ij}. Hodnota k_{ij} náležící k hraně h_{ij} vyjadřuje dobu trvání činnosti mezi uvedenými uzly. (Pro označení $NMK_{i,j}$ se užívá symbol $t_j^{(0)}$).

$$NMK_{i,j} = NMZ_{i,j} + k_{i,j} \tag{3.1}$$

- $NPK_{i,j}$ - *nejpozději přípustný konec činnosti* probíhající mezi u_i a u_j je informace o tom, kdy nejpozději musí být ukončena činnost v u_j, aby byl dodržen vypočtený (stanovený) termín ukončení celého projektu. (Pro označení $NPK_{i,j}$ se užívá symbol $t_j^{(1)}$).

- $NPZ_{i,j}$ - *nejpozději přípustný začátek činnosti* počínající v u_i a končící v u_j určuje, kdy nejpozději musí být dílčí činnost v u_i zahájena, aby bylo možno celý projekt ukončit ve vypočteném (stanoveném) termínu. ($NPZ_{i,j}$ se označuje $t_i^{(1)}$).

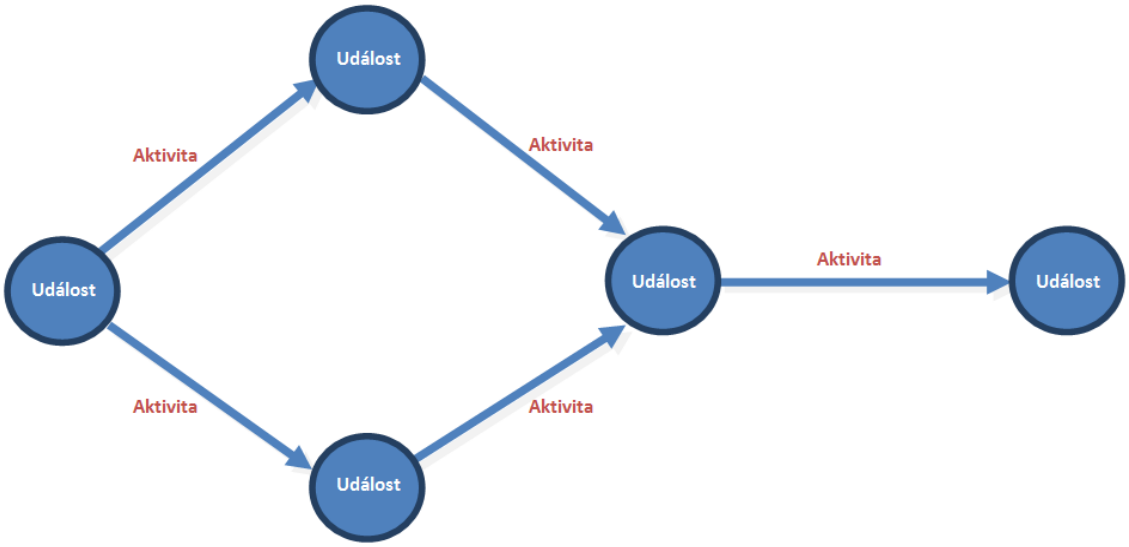
$$NPZ_{i,j} = NPK_{i,j} - k_{i,j} \tag{3.2}$$

V *první fázi* vypočteme NMZ a NMK pro dílčí činnosti a s jejich pomocí určíme nejdříve možný termín ukončení celého projektu. V této fázi procházíme graf od počátečního ke koncovému uzlu a hledáme v grafu nejdelší cestu mezi u_0 a u_j - její délka je totožná s nejkratší možnou dobou realizace projektu. V *druhé fázi* metody CPM vypočteme NPK a NPZ jednotlivých činností, s jejich pomocí pak stanovíme **kritické činnosti** a **kritickou cestu v grafu**. V této fázi metody procházíme síť ve směru od koncového uzlu u_j k počátečnímu u_0. Ve *třetí fázi* je možno pro každou z dílčích činností vypočítat kolik času máme k dispozici na jejich provedení. Na závěr řešení problému je vhodné vytvořit názornou představu o tom, které z dílčích činností probíhají souběžně a které naopak mohou (nebo musí) být uskutečněny následně. (11)

3.5.2 Stochastická metoda PERT

Tato metoda, která bude dále využita, vznikla v roce 1958 při vývoji vojenských raket odpalovaných z ponorek, kdy tato metoda pomohla zásadně zkrátit celý projekt. Metoda PERT pak byla dále rozvíjena, například o metody GERT, MAPS, RAMPS. (11)

Metoda PERT používá síťový diagram, který se skládá z událostí (uzlů), které musí být vytvořeny k dosažení určitých stanovených cílů. U této události musí být stanoven přesný čas, ve kterém má být plán splněn. To indikuje důležitost času a nepotřebuje proto nějaké další dodatečné zdroje pro sestrojení PERT diagramu. PERT využívá orientované síťové



Obrázek 3.4: Hranově ohodnocený síťový diagram PERT

diagramy událostí, které jsou spojeny šipkami a představují aktivity (činnosti) aby nastala námi projektovaná událost. (13)

Událost představuje uzel, kterého má být dosaženo pomocí aktivit představující činnosti. Aktivita představuje čas potřebný k přesunu z jedné události nebo činnosti do další, což je determinováno směrem šipek v grafu. PERT systém je preferovaný pro ty projekty nebo operace, které se neopakují, případně pro ty, u kterých je velmi obtížné určit přesný čas trvání události. Je vhodný u projektů v oblastech, kde management nemá přímé předchozí zkušenosti v dané problematice. Metoda je vhodná pro projekty, které se jednou aplikují a neustále se opakují. Příkladem mohou být projekty z oblasti výzkumu či vývoje. (13)

Jednotlivé události, jinak též dále činnosti je nutné časově ohodnotit. Trvání každé činnosti je považováno za náhodnou veličinu s určitým rozdělením pravděpodobností. Jednotlivé činnosti projektu jsou ohodnoceny stochasticky, ve třech časových odhadech:

- otimistický odhad trvání (značený písmenem a),
- nejpravděpodobnější odhad trvání činnosti (značený písmenem m),
- pesimistický odhad trvání činnosti (značený písmenem b).

Časovou analýzu pomocí metody typu PERT lze provést dvěma postupy:

- metoda Monte Carlo,
- převod na deterministický model.

Při použití metody **Monte Carlo** je však nutnou podmínkou implementace generátoru náhodných čísel v počítači, který náhodně vybere časové ohodnocení konkrétní činnosti

v rámci intervalu <a, b>. Jde o stochastickou metodu používající pseudonáhodná čísla. Nachází využití při výpočtu určitých integrálů nebo řešení diferenciálních rovnic. Z obecného hlediska postupem při řešení problému pomocí této metody je určení střední hodnoty veličiny, která je pak výsledkem náhodného děje. Pomocí vytvořeného počítačového modelu tohoto děje a po provedení dostatečného množství simulací lze provést klasické výpočetní metody, jako je např. průměr, směrodatná odchylka. (14)

Převod na **deterministický model** lze použít v opačném případě, kdy nechceme provádět mnohočetné simulace nebo nemá tato metoda vzhledem k danému problému praktické využití. Pokud se stochastický model převede na deterministický, je možné pak daný problém řešit pomocí modelu nejkratší cesty v grafu, respektive CPM metodou. Řešení ale není naprosto shodné s tímto modelem. Síťový diagram je řešen shodně dle CPM, avšak jednotlivé činnosti jsou ohodnoceny stochasticky, jak bylo uvedeno výše, a to na optimistický, nejpravděpodobnější a pesimistický odhad trvání činností. Výpočet těchto veličin je pak následující:

- Očekávané trvání činnosti:

$$t_c = \frac{a + 4m + b}{6} \tag{3.3}$$

- Rozptyl trvání činnosti:

$$D_{t_c}^2 = \left(\frac{b - a}{6}\right)^2 \tag{3.4}$$

- Směrodatná odchylka:

$$\sqrt{D_{t_c}} = \frac{b - a}{6} \tag{3.5}$$

Po výpočtu dle vzorců 3.1-3.3 je dalším krokem časová analýza provedená stejným způsobem jako metoda CPM. V rámci této analýzy je použito hranově definovaných síťových grafů s konjunktivně deterministickou interpretací uzlů, což znamená, že uzel může být realizován jen tehdy, pokud jsou realizovány všechny činnosti, které v tomto uzlu končí. Realizace tohoto uzlu je podmínkou pro zahájení realizace všech dalších činností, které z uzlu vystupují. Výsledkem časové analýzy pomocí této metody PERT je určení kritické cesty s maximální střední hodnotou trvání. (14)

Pravděpodobnost splnění termínu dostaneme pomocí vzorců:

$$P(T \leq T_p) = F\left(\frac{T_p - T_e}{\sqrt{D_{t_c}}}\right) \tag{3.6}$$

$$F\left(\frac{T_p - T_e}{\sqrt{D_{t_c}}}\right) = F(u) \tag{3.7}$$

Kde je:
T_p - plánovaný termín ukončení celého projektu,
T_e - očekávaný termín realizace celého projektu,
$F(u)$ - hodnoty distribuční funkce normálního rozdělení.

Pokud je dosažena pravděpodobnost splnění plánovaného termínu v rozsahu 40 - 60 %, je realizace projektu splněna na požadované úrovni. Hodnoty přesahující 60 % naznačují nadbytečné využívání zdrojů a hodnoty menší jak 40 % vypovídají naopak o nutnosti lepšího zajištění činností umístěné na cestě do daného uzlu. Tyto problémy lze řešit například zlepšením organizace práce, optimalizace zdrojů, efektivním využitím času a podobně. Pokud se v modelu vyskytne více kritických cest, měla by se věnovat pozornost více kritické cestě s největším rozptylem. (15)

3.6 Hodnocení informačního systému

Obsahem této kapitoly je metoda, kterou budeme hodnotit efektivitu informačního systému na základě předložených dotazníků v daném podniku. Tato metoda se skládá ze dvou částí, které nám pomohou odhalit skryté problémy z hlediska informačních systémů. Na základě získaných výsledků určíme různá opatření k eliminaci všech možných ne dostatků. Obsahem první části je výzkum měření efektivnosti informačních systémů, obsahem druhé části je využití metody HOS. V první části budou dotazníky vyplněny zaměstnanci podniku, kteří s informačním systémem běžně pracují. V druhé části bude dotazník týkající se metody HOS vyplněn pouze jedním pracovníkem, který v podniku plní funkci nadřízeného. Všechny dotazníky i vyhodnocení bude provedeno pomocí ZEFIS. Veškeré dotazníky jsou vyplněny elektronickou formou, cestu k ni naleznou zainteresovaní lidé v podniku pomocí rozeslaného elektronického odkazu.

3.6.1 Efektivnost informačního systému

Výsledky z vyplněných dotazníků se porovnají s výsledky referenční databází, které jsou využity k odhalení nedostatků informačního systému. Na základě této analýzy jsou navržena případná zlepšení a nápravná opatření pro IS SAP, dále je pak vybrán kritický nedostatek, kterým se tato práce nadále zabývá a hledá se řešení k nápravě tohoto nedostatku. (10)

3.6.2 Posouzení osmi klíčových oblastí

Metoda posouzení osmi klíčových oblastí je těsně spjata s posouzením efektivnosti informačního systému, pouze respondenty jsou v tomto případě vedoucí pracovníci, přičemž samotná metoda posouzení efektivnosti informačního systému, dotazníky vyplňují všichni zaměstnanci (včetně managementu), kteří s posuzovaným informačním systémem pracují. Na základě osmi oblastí je posouzena vyváženost informačního systému, jejíž porušení povede k neúměrnému zvýšení nákladů. (10)

Mezi osm posuzovaných oblastí patří:

1. **Hardware** - technické vybavení podniku.
2. **Software** - programového vybavení, jeho funkce, snadnost používání a ovládání.
3. **Orgware** - pravidla pro práci s informačními systémy, doporučené pracovní postupy, bezpečnostní pravidla.
4. **Peopleware** - zkoumaní uživatelů informačních systémů a pohled na jejich povinnosti.
5. **Dataware** - správa, bezpečnost a dostupnost dat.
6. **Zákazníci** - uživatelé informačního systému.
7. **Dodavatelé** - fyzické nebo právnické osoby, které zajišťují provoz IS.
8. **Management** - řízení IS, kontrola dodržování pravidel a podpora koncovým uživatelům IS. (10)

3.6.3 Hodnocení výsledků

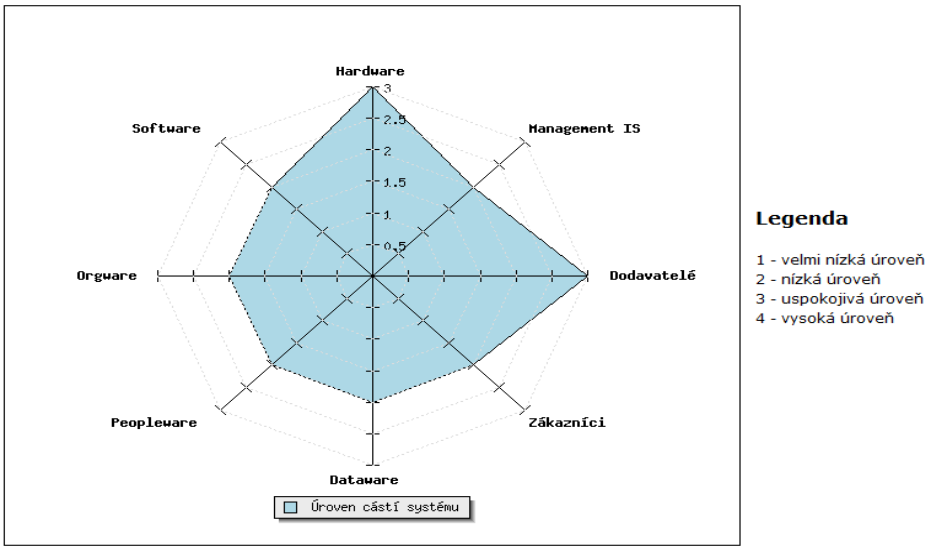
Každá oblast je ohodnocena podle číselné stupnice: 1- špatná, 2 -spíše špatná, 3 - spíše dobrá 4 - dobrá. Záleží na konečném hodnocení všech těchto oblastí, optimálním výsledkem je vyváženost všech oblastí, jinými slovy všechny oblasti musí být stejně ohodnoceny, a to nejlépe známkou dle bodu 4. Pokud jedna z oblastí obsahuje nižší hodnocení, pak je úroveň informačního systému determinována právě tímto nejslabším článkem. Takovým příkladem může být špičková reprosoustava. V případě uživatele, který si takovou soustavu pořídí, kde komponenty se pohybují v řádech desetitisíců korun, ale reprosoustavu pořídí v řádech stokorun, pak je příznačné, že úroveň celé soustavy domácího kina je logicky snižována levnou reprosoustavou, která nevyužije celý potenciál multimediálního centra. Lze připustit odlišení úrovně zkoumaných úrovní maximálně o 1 stupeň za předpokladu, že je toto odlišení nutné. (10)

Příkladem je obrázek 3.5, kde je patrná nevyváženost IS. Většina oblastí dosahuje úrovně 2, avšak management IS a dodavatelé úrovně 3. Jedná se o celkově nevyváženou úroveň informačního systému a dle číselné stupnice je to informační systém se spíše špatnou úrovní, jak je zobrazeno na obrázku 3.6. (10)

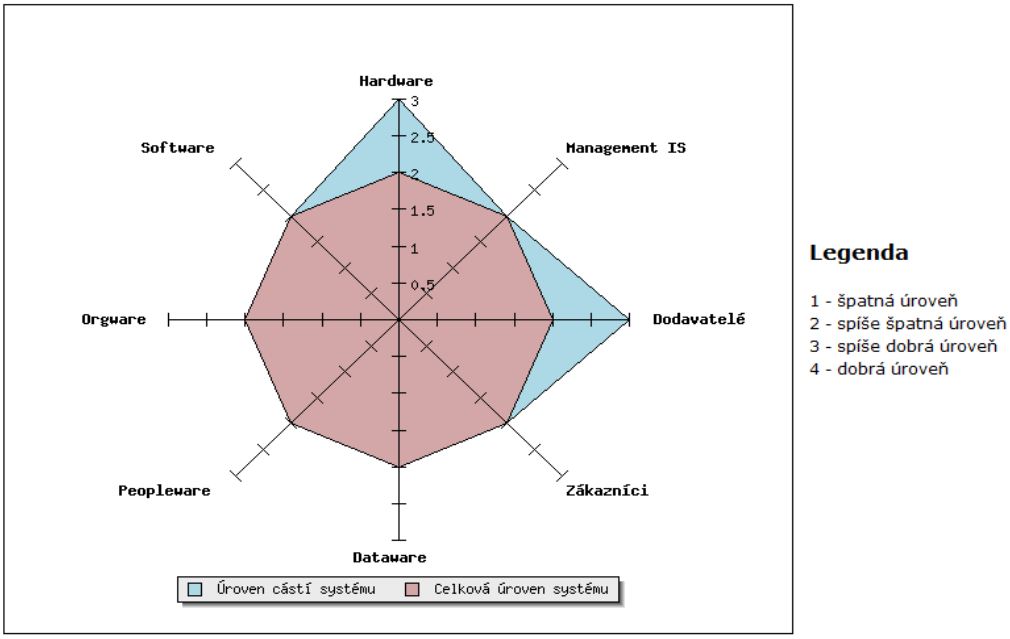
Aby se zabránilo takovým případům a vzniku nadbytečných nákladů na úkor nevyváženosti informačního systému, je doporučeno všechny oblasti vyvážit do harmonického stavu. Jedině tak lze hovořit o optimálním informačním systému, který funguje efektivně. (10)

Optimálně vyvážený informační systém je zobrazen na obrázku 3.7 pomocí červené čáry znázorňující optimum. (10)

Pokud jsou oblasti IS nevyvážené nebo nedosahují doporučené hodnoty, nabízí řešení další strategie:



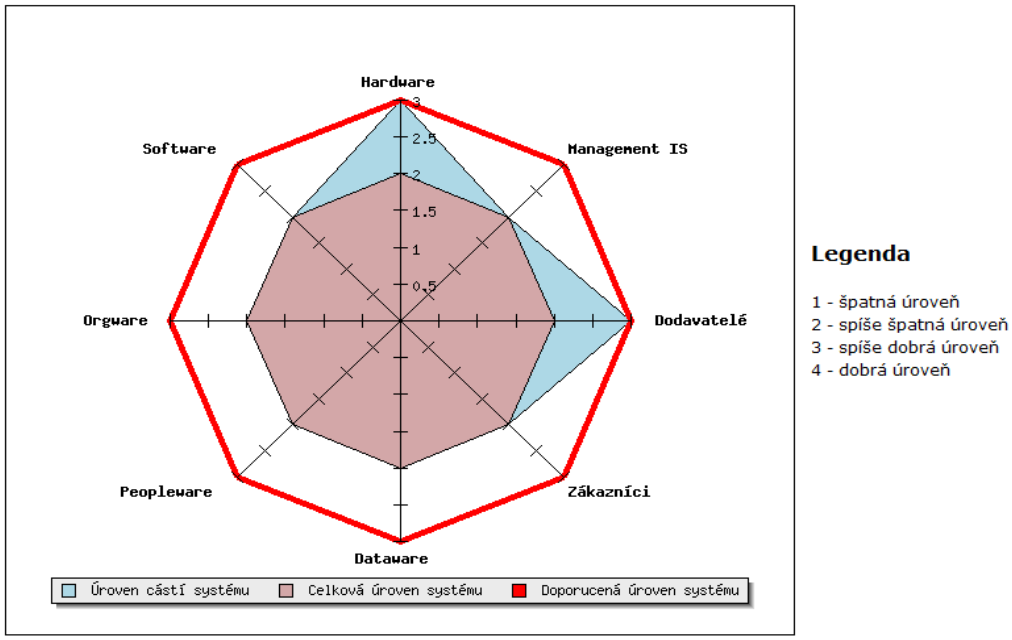
Obrázek 3.5: Nevyvážené jednotlivé oblasti



Obrázek 3.6: Spíše špatná úroveň informačního systému

- **Strategie útlumu** - cílem je snížit úroveň oblasti na úroveň ostatních oblastí nižší úrovně. Dochází k zastavení investicí do této oblasti, které jsou pak rozděleny mezi ostatní oblasti.

- **Strategie udržení současného stavu** - tato strategie udržuje optimální stav informačního systému, kdy jsou oblasti vyváženy a dosahují požadované doporučené



Obrázek 3.7: Doporučená úroveň

hodnoty na číselné stupnici. S touto strategií jsou spojeny určité náklady na údržbu do doby, kdy je nutno investovat do obnovy hardware nebo software.

- **Strategie zlepšení, rozvoje** - opak strategie útlumu, podnik investuje do oblasti, která je pod úrovní ostatních oblastí, přičemž to nemusí být nákladná investice, pokud se jedná například o organizační změny nebo zlepšení procesů. (10)

3.7 Bezpečnostní politika

Problematika bezpečnosti IS bývá často opomíjená v mnoha podnicích. Může to být problém nejen malých podniků, začínajících podniků, ale i velkých podniků, pokud zde neexistují zodpovědné osoby k tomuto účelu určené. V dnešní době se bezpečnost staví do role aktuálních témat, které není radno opomíjet, pokud podnik nechce utrpět nějakou škodu. Celá oblast bezpečnostní politiky spočívá v mnoha krocích a činnostech. Mezi ty hlavní patří objektová bezpečnost, bezpečnost a ochrana zdraví při práci a informační bezpečnost. Všechny tyto aspekty určitým způsobem souvisí s informačním systémem v podniku, které je nutné mít pod kontrolou, pokud má celý informační systém fungovat bez zbytečných ztrát, např. díky výpadku systému, výpadku IS apod. (17)

Objektová bezpečnost se zabývá řešením ochrany budov a prostor, patří sem jejich ostraha včetně zajištění požární a další ochrany. **Bezpečnost a ochrana zdraví při práci** (BOZP) se zabývá podmínkami a charakterem činností podniku za účelem zajištění ochrany zdraví pracovníků. **Informační bezpečnost** se pak zabývá ochranou informačních aktiv podniku. (17)

Aktivum je vše, co má pro jednotlivce nebo podnik nějakou hodnotu, která by mohla být degradována působením určité hrozby. Z toho plyne, že hlavní charakteristika pro aktiva je jejich **hodnota**. Hodnota aktiv se stanovuje pomocí subjektivního vnímání důležitosti aktiva nebo objektivním vnímání jeho ceny, nebo kombinace obou přístupů. Tato hodnota je určena úhlem pohledu hodnocení, je tedy relativní. Další charakteristika aktiv je **zranitelnost**. (24)

Definice zranitelnosti z pohledu aktiv je citlivost aktiva na působení hrozby. Z hlediska praxe se musí počítat s tím, že každé aktivum v podniku má nějaké zranitelné místo, má nějakou slabinu, která může být zneužita za účelem způsobení nějaké škody nebo ztráty. Takové zranitelné místo může být fyzické, přírodní, technologické, fyzikální nebo lidské. Pro každé takové aktivum by se měla určit citlivost (náchylnost) a kritičnost (důležitost). (17)

Zranitelné místo je pro každý systém hrozbou („threat“), což lze charakterizovat jako slabé místo, které lze využít k útoku na dané aktivum. Tento útok označujeme termínem **bezpečnostní incident** („security incident“), což je porušení definovaných pravidel a postupů při provozování IS/ICT. Řadící se mezi ně i jen pokusy o tato porušení, dále i jakákoliv událost vedoucí k ohrožení definovaných bezpečnostních vlastností. Zranitelná místa a hrozby vyhledávají a využívají **útočníci** k vedení svého útoku. Útočník může být osobou, která se může vyskytovat uvnitř podniku nebo své kroky může podnikat zvenčí, ať už je to útok cílený nebo neuvědomělý. V případě uvědomělého útoku rozlišujeme několik druhů útočníků:

- *Hacker* - útok na podnik je pro něj výzva a způsob získání prestiže.
- *Vyzvědač* - útoky jsou provedeny za účelem zisku informací sloužících pro různé politické účely.
- *Terorista* - útoky jsou vedeny za účelem vyvolání obavy nebo strachu.

- *Kriminálník* - cílem útoku je osobní finanční zisk.
- *Vandal* - důvod útoku je poškození nebo zničení systému.
- *Cracker* - osobou vedoucí útok je s největší pravděpodobností programátor, který proniká do systémů chráněných autorským zákonem za účelem jejich krádeže.
- *Phracker* - útok za účelem získání bezplatného přístupu k telefonním službám.
- *Phreaker* - cílem je přístup k dalším počítačům s využitím telekomunikačních informací. (24)

Každá hrozba nebo zranitelné místo aktiv podniku zvyšují riziko vzniku bezpečnostního incidentu vyjádřené jeho úrovní pomocí hodnoty rizika. Aby bylo těmto rizikům předejito nebo alespoň výše rizika minimalizována, je třeba vybrat určitá protiopatření přiměřená hodnotě chráněných aktiv. S těmito pravidly souvisí tzv. **referenční úrovně rizika**, jejichž hladina by měla být taková, aby dopad hrozby byl zanedbatelný. (17)

Aby byla všechna potencionální rizika minimalizována, musí dojít k implementaci protiopatření. Dle národní strategie informační bezpečnosti ČR by se měl každý IS u nás řídit i tzv. **bezpečnostními požadavky**, což vychází z celé řady standardů, norem, zákonů a nařízení. Obecně je lze charakterizovat jako **zachování důvěrnosti**, kdy přístup k aktivům podniku mají pouze pověřené subjekty, dále pak **zachování dostupnosti**, kdy pověřené osoby mohou na své vyžádání provést činnosti a není jim odepřen k činnosti přístup a zachování integrity, aby bylo zabráněno neautorizovaným osobám provádět změny aktiv, nepovolenou činností nebo nekompletním provedením změn. (24)

Abychom zajistili výše uvedené bezpečnostní požadavky, je nutné sledovat a ovlivňovat zajištění prokazatelnosti, kdy musí být umožněno nejen vysledovat jakoukoliv akci provedenou v systému, ale i identifikovat původce takové akce, dále pak zajištění nepopíratelnosti umožňuje situaci, kdy subjekt nemá možnost odmítnout svoji účast na provádění nějaké akce a zachování spolehlivosti, které by mělo umožnit reálné chování systému takovým způsobem, aby bylo konzistentní s chováním systému dle dokumentace. (17)

3.7.1 Přístup k řešení bezpečnosti

Obrázek 3.8 znázorňuje základní přehled o obsahu řešení bezpečnosti IS/ICT. Tyto činnosti jsou součástí skupiny **řízení rizik**. K dalším činnostem se řadí kontrola a audit bezpečnosti, monitorování, hodnocení, certifikace a akreditace bezpečnosti IS/ICT. Bezpečnostní politika pak definuje jaký stupeň zajištění bezpečnostních požadavků má být aplikován na konkrétní IS/ICT. (24)

Bezpečnostní politika je souhrn pravidel a zásad, s jejichž pomocí podnik chrání svá aktiva. Musí být neustále aktualizována vzhledem ke změnám prostředí a může obsahovat:

- proceduru vyhodnocení účinnosti politiky vedoucí k provedení její změny,
- objasnění způsobu uskutečňování a vynucování bezpečnostních opatření,

Obrázek 3.8: Obsah řešení bezpečnosti IS/ICT

- politiku přípustného užívání aktiv,
- specifikaci vzdělávacího procesu svých zaměstnanců v oblasti ochrany aktiv.

Samozřejmě se bezpečnostní politika může lišit v každém podniku, musí se totiž přizpůsobovat podmínkám, které se v podniku vyskytují. Je možné definovat čtyři obecné typy bezpečnostní politiky:

1. **Promiskuitní** - pravidla neexistují, nebo existují, ale ve svých pravidlech nikoho neomezují a povolují subjektům realizovat vše, tedy i to, co by neměli standardně konat.

2. **Liberální** - ve svých pravidlech umožňuje realizovat vše, až na výjimky, které jsou explicitně vyjmenované.

3. **Opatrná** - pravidla zakazují vše s výjimkou toho, co je explicitně vyjmenováno.

4. **Paranoidní** - stanovená pravidla zakazují vše, co je potencionálně nebezpečné, tedy i to, co by nemuselo být explicitně zakázáno. (17)

3.7.2 Potencionální hrozby

Hrozby, které mohou ohrozit místo aktiv, se dělí na přírodní a fyzické, technické, technologické a lidské. Přírodní a fyzické hrozby mohou být živelné pohromy nebo nehody, jako jsou výpadky elektrického proudu, požáry apod. Mezi technické hrozby se řadí poruchy nosičů a počítačů nebo sítí. Poruchy způsobené software, např. viry apod. se řadí mezi technologické hrozby. Lidské hrozby se dělí na úmyslné a neúmyslné. Úmyslné hrozby mohou být děleny na působící zvenčí, kam lze zařadit teroristy, hackery, špionáž atd. a působící zevnitř, kam lze řadit lidské faktory jako zlomyslnost, chamtivost, zneuznání. (24)

Mezi **úmyslné** lidské hrozby patří *odposlech* pomocí vyhledávání hesel pomocí trójského koně, útoku hrubé síly, slovníkového útoku nebo útoku na heslo související s uživatelem, *modifikace* obsahu určitých transakcí či změna uložených informací, *podvody* za účelem získání významných citlivých informací. *Odmítnutí, popření* útoku, při kterém jedna strana odmítá svoji účast na provedené transakci, což pak může vyústit k odstoupení od smlouvy z důvodu problémů zpracování citlivých dat. Tyto útoky jsou nazvány termínem „Denial of Service“ (DoS). Mezi známé útoky DoS patří E-mail bomba, kdy e-mail server je zatížen abnormálním množstvím zaslaných zpráv a dojde k obrovskému zahlcení síťového spoje a zaplnění paměťových kapacit. Další DoS může být Ping of Death, který spočívá v zasílání abnormálně velkých paketů[11] na vybraný server. Zombies jsou druhy programů, které jsou nainstalovány do hostitelského programu a pak následně využity k útoku na tento počítač. (24)

Mezi neúmyslné lidské hrozby, které mohou vyplynout i z neznalosti, nedbalosti či omylu, lze zařadit např. prozrazení tajných informací, upravení aktiv subjektem, kdy dojde k poruše integrity dat, zničení informací a bránění v dostupnosti IS autorizovaným subjektům. Více jak padesát procent hrozeb je neúmyslných. (17)

Hogging je druh DoS útoku, kdy jsou spotřebovány veškeré zdroje daného zařízení (RAM, čas procesoru atd.). SYN floading užívá vlastnosti TCP[12] při navazování spojení, kdy je vyžadován velký počet žádostí o spojení, které je ale před vlastním uskutečněním spojení útočníkem ukončeno. Útočníci ke své nekalé činnosti využívají často škodlivé programy, tzv. *škodlivé kódy* (malware, malicious software), jejichž úkolem je poškodit aktiva v podniku. Patři mezi ně viry (má buď jednu část, která škodí nebo druhou která se množí nebo jejich kombinace), poplašné zprávy (plané hrozby rozesílané nezkušenými uživateli, někdy je nazýván i termínem spamming[13]), spyware (sledování činnosti počítače a uživatele) a další parazitující programy. (17)

3.7.3 Protiopatření

Neexistuje žádné univerzální protiopatření, které by dokázalo informační systém komplexně ochránit. Konkrétní řešení je zaměřeno na minimalizaci daného rizika. Jaké protiopatření zvolit, to závisí na činnosti analýzy rizik. Existují dva přístupy k protiopatření

[11] Blok dat přenášený v počítačových sítích

[12] Transmission Control Protocol - pomocí TCP lze přenášet mezi PC v síti data

[13] obtěžující nevyžádaný e-mail

v podniku. (17)

Podle vztahu protiopatření vůči průběhu bezpečnostního incidentu:

- **preventivní** - účelem je minimalizace příčin možného vzniku bezpečnostního incidentu,
- **dynamická** (proaktivní) - účelem je minimalizace možných dopadů aktuálně probíhajícího bezpečnostního incidentu, zahrnující včasné zachycení vzniku takového incidentu,
- **následná** (reaktivní) - účelem je minimalizace možných dopadů uskutečněného bezpečnostního incidentu. (24)

Podle formy protiopatření:

- **administrativní** - účelem je nastavení administrativních a organizačních pravidel vedoucí k minimalizaci vzniku a průběhu bezpečnostních incidentů, včetně jejich dopadů,
- **fyzická** - cílem je fyzicky zajistit aktiva, aby byla minimalizována pravděpodobnost vzniku a průběhu bezpečnostních incidentů, včetně jejich dopadů,
- **technologická** - aktiva by měla být zajištěna technologicky takovým způsobem, aby byla minimalizována pravděpodobnost vzniku a průběhu bezpečnostních incidentů, včetně jejich dopadů. (17)

Jako příklad protiopatření je možné uvést doručení zprávy adresátovi bez zásahu útočníka, tedy aby tato nebyla po jejím uložení změněna. K tomu je vhodné využít např. **digitální podpis**, který je dodatkem ke zprávě. Využívá se k tomu asymetrické šifrování a prostředky tvorby výtahu zprávy. V asymetrickém šifrování využíváme dvojice klíčů, kdy je jeden z nich označovaný jako veřejný klíč a druhý soukromý klíč. Oba klíče jsou vygenerovány speciálními prostředky. Prostředky pro tvorbu výtahu zprávy je pomocí matematických operací ze vstupu libovolné délky výstup o konstantní délce, přičemž obrácený postup není možný. Mezi další protiopatření patří využití prvku **firewall**, který spočívá v oddělení prostředí důvěryhodné sítě podniku (zpravidla sítě LAN[14]) od nedůvěryhodného prostředí (za hranicí podniku). Úkolem firewallu je řízení provozu a rozhodování, jak bude naloženo s příchozími a odchozími požadavky. V neposlední řadě je velmi důležitá **ochrana před škodlivými kódy**. (24)

K bezpečnostnímu incidentu může dojít například v případě otevření přílohy k e-mailové zprávě, zapsané HTML kódy využívající JavaScript, instalované programy z nedůvěryhodných zdrojů apod. K ochraně proti škodlivým kódům může sloužit nejen firewall, ale hlavně antivirový program, nejlépe však obě ochrany v kombinaci tzv. „smart security“ programy, jako je například NOD32. Mezi další antivirové programy patří AVG, Avast!, Kaspersky Lab, Norton, Microsoft Security Essentials atd. U každého IS musí fungovat i **zálohovací**

[14]Local Area Network - lokální síť, místní síť

systém schopný reagovat na rostoucí objemy dat, umět pracovat v různorodém prostředí s heterogenním typem dat, tvořit klony zálohovaných dat pro potřeby uložení na jiném místě s možností centralizované správy. (17)

3.7.4 Mezinárodní bezpečnostní standard

Norma ISO/IEC 27005 definuje aktivum jako něco, co má nějakou hodnotu pro podnik a vyžaduje v podniku ochranu. Popis identifikací aktiv v této normě navrhuje, aby bylo s každým aktivem nakládáno na úrovni ohodnocení rizik, což by mělo být každým vlastníkem nebo managementem v podniku identifikováno u každého aktiva. Výstupem této normy je pak seznam aktiv ohodnocených na úrovni managementu rizik a seznam podnikových procesů odkazujících se na tato aktiva a jejich důležitost. (20)

3.7.5 Identifikace a ohodnocení aktiv

Každý podnik je závislý na celé řadě svých činností, na svých zaměstnancích a dostupných hmotných i nehmotných aktivech. Nezbytnou úlohou managementu podniku je tato aktiva chránit. Každé aktivum podniku má svoji hodnotu a je pro podnik kritickým. Identifikace aktiv je založena na vytvoření seznamu aktiv, která patří do námi zvolené hranice bezpečnosti. Mezi takové skupiny aktiv patří **informace** (jedná se o smlouvy, podnikové strategie, obchodní informace apod.), **hmotný** a **nehmotný majetek**. Ohodnocení aktiv by se mělo řídit podle významu, důležitosti a vyčíslení ztráty pro podnik. Ohodnocení fyzických aktiv není příliš obtížné, protože jeho hodnotu je možné určit na základě pořizovací ceny nového aktiva, je však nutné aktivum ohodnotit i z hlediska důležitosti aktiva pro daný podnik. Nehmotná aktiva se z finančního hlediska velmi těžko oceňují, výsledky mohou vést ke špatným závěrům. (18)

Pro **ohodnocení aktiv** se používá škála 1 až 5, přičemž nejdůležitější jsou aktiva označena číslem 5. Jako typ skupiny aktiv se ohodnocuje nejčastěji skupina informace, hardware, software a služby. Po ocenění aktiv a určení hodnot aktiv následuje **identifikace hrozeb** a **zranitelnosti**. Pro ohodnocení pravděpodobnosti hrozby je opět použita škála 1 až 5, kdy nejpravděpodobnější hrozba je ohodnocena číslem 5. V tomto případě je si nutno uvědomit, že jedna hrozba může využít více zranitelností a stejně tak i jednu zranitelnost může využít více hrozeb. (19)

3.7.6 Řízení rizik

Správné řízení rizik umožní stanovení rozsahu projektů, vytvořené realistického časového plánu a odhadu nákladů. Efektivní řízení pak umožňuje snížení počtu problémů a urychlení jejich řešení. Řízení rizik lze chápat i jako investici v podobě nákladů, která se odvíjí od zájmu organizace vynaložit náklady na aktivity řízení rizik, které by v žádném případě neměly přesahovat potencionální přínosy. (23)

3.7.6.1 Analýza rizik

Pro analýzu rizik v podniku se používá matice aktiv, hrozeb a zranitelností. K této analýze se používá tabulka, kde se doplňují identifikovaná aktiva, identifikované hrozby a jejich pravděpodobnosti. K tomuto kroku lze využít i ISO/IEC 27005, kde je mj. uveden i katalog hrozeb. Dalším krokem je posouzení zranitelnosti jednotlivých aktiv (skupin aktiv) pomocí jednotlivých hrozeb a jejich doplnění do tabulky. V případě, že mezi hrozbou a aktivem není vazba, zůstane daná buňka prázdná. (29)

Při určování druhů rizik, které se mohou v praxi objevit, si lze uvést pár příkladů. Tržní riziko popisuje riziko z hlediska možnosti konkurence výrobku nebo služby na trhu, vlivu poptávky apod. **Finanční rizika** zvažují veškeré možnosti podniku z hlediska investic do nového projektu a doby návratnosti této investice. **Technologická rizika** posuzují technickou zvládnutelnost projektu. Mezi takové aspekty může patřit moderní technologie, funkčnost technologie, včasnost atd. **Lidská rizika** zahrnují otázky jako dostatek potřebných pracovníků v podniku, dobu náboru, znalosti, management, praxi apod. **Strukturální a procesní rizika** mapují stupeň změny nového projektu zavádění do uživatelské oblasti, uspokojení různých skupin uživatelů, úplnost procesů ke zdárnému dokončení projektu. (23)

Posledním krokem analýzy rizik je výpočet míry rizika, k tomu slouží vzorec 3.6, kde R je míra rizika, T je pravděpodobnost vzniku hrozby, A je hodnota aktiva a V je zranitelnost daného aktiva:

$$R = T * A * V \tag{3.8}$$

Po analýze rizik zbývá stanovit hranice pro nízká (přijatelná), střední a vysoká rizika, což může být provedeno managementem nebo specialisty, kteří v podniku pracují. (29)

3.7.6.2 Registr rizik

Registr rizik je dokument, ve kterém jsou uvedeny výsledky různých procesů řízení rizik, často bývá prezentován ve formě tabulky nebo tabulkového listu. Rizikové události jsou v tomto případě nejisté okolnosti, které mohou buď ohrozit celý projekt nebo mu prospět. Z tohoto hlediska rozeznáváme pozitivní (např. zkrácení doby projektu) a negativní rizika (např. soudní spor). Registr rizik je tedy zaznamenaný v tabulce, která obsahuje atributy, jako jsou:

- *Identifikační číslo každé rizikové události* - pokud chceme rychle vyhledat riziko, pomůže nám k tomu vhodný systém označení, může to být číslo, kombinace písmen a čísel nebo jen písmena, záleží na projektantovi.
- *Hodnocení dané rizikové události* - stupnice určující míru rizika, číslo 1 představuje nejvyšší míru rizika.
- *Název rizikové události* - zvolíme libovolný název.

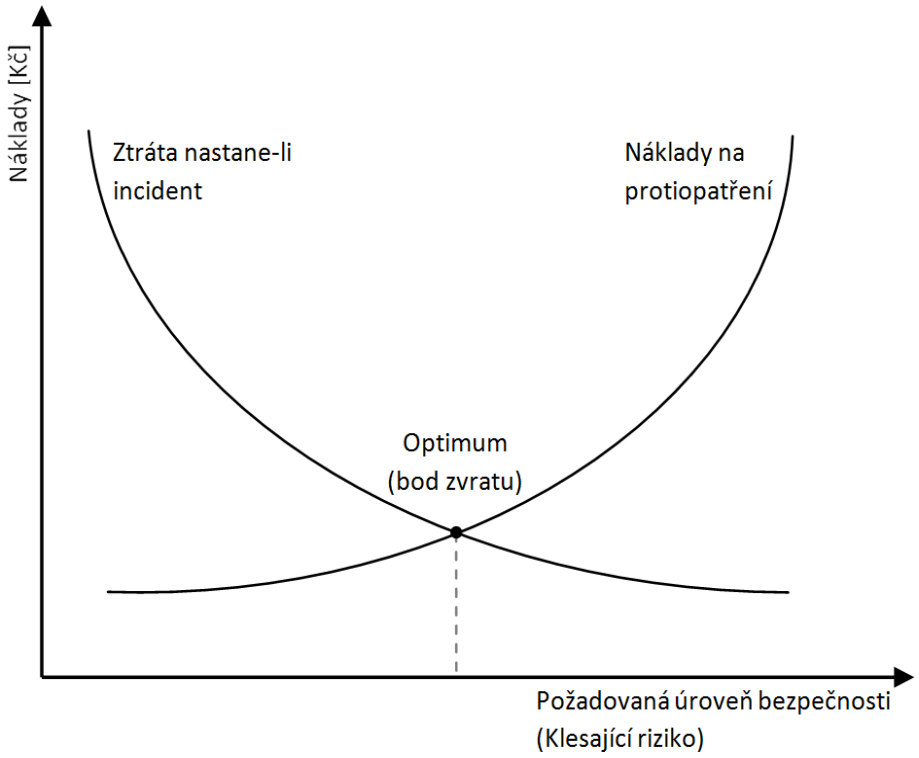
- *Popis rizikové události* - zde je uveden podrobnější popis rizikové události.
- *Kategorie, do které tato riziková událost spadá* - subjektivní zařazení rizikové události do určité skupiny, tzv. kategorie.
- *Prvotní příčina rizika* - hledání potencionálního zdroje vzniku rizika.
- *Spouštěče dané rizikové události* - indikátory skutečného vzniku rizikové události. Není vyloučeno, že zdokumentování symptomů neodhalí další rizikové události.
- *Potencionální reakce na jednotlivá rizika* - předem vymyšlené návrhy řešení pravděpodobných bezpečnostních incidentů.
- *Vlastník rizika* - osoba, která je zodpovědná za dané riziko.
- *Pravděpodobnost vzniku rizika* - nízká, střední nebo vysoká pravděpodobnost.
- *Dopady případného vzniku rizika pro řešený projekt* - může mít nízký, střední nebo vysoký dopad na úspěch projektu.
- *Stav rizika* - popisuje aktuálně zaujaté stanovisko k danému riziku. (23)

3.7.6.3 Způsoby potlačení rizik

S výskytem rizik v podniku je nutno počítat. Každé riziko je možné minimalizovat. Ale ochrana proti riziku a pokus o vyhnutí se bezpečnostnímu incidentu je otázkou nákladů, tzn. čím vyšší míra zabezpečení, tím vyšší náklady pro podnik. Pro podnik to znamená zvážit cenu aktiva a možný náklad zvoleného protiopatření. Nejlepší způsob, jak dosáhnout optimálního zabezpečení proti riziku, je dostat se do bodu, kdy budou náklady protiopatření stejné jako případně vzniklá ztráta (hodnota aktiva). Útočník pak bude muset vynaložit více úsilí, než jaký mu útokem získané aktivum přinese užitek, jak je znázorněno v grafu na obrázku 3.9. (21)

Mezi strategie řešení pozitivních rizik patří využití rizika, sdílení rizik, posílení rizika a přijetí rizika:

- **Využití rizika** - jedná se o jakoukoliv činnost vedoucí k situaci, kdy kladné riziko nastane. Příkladem může vytváření dobrého veřejného mínění.
- **Sdílení rizika** - přenesení rizika na další subjekt.
- **Posílení rizika** - posílení příležitosti, jinými slovy činnost, vedoucí k přilákání dalších potencionálních zákazníků.
- **Přijetí rizika** - lhostejné postavení k rizikům, ať už je to za situace nemožnosti dané rizika ovlivnit nebo projektový tým s danými riziky nechce nic dělat. (23)



Obrázek 3.9: Analýza nákladů a přínosů

Máme několik možných řešení negativních rizik, a to redukci, zadržení, transfer a retenci:

- **Redukce rizika** - činnosti vedoucí ke snížení pravděpodobnosti, negativním důsledkům, nebo obojího, spojené s rizikem.
- **Zadržení rizika** - veškerá rozhodnutí, která vedou k eliminaci situace obsahující riziko.
- **Transfer rizika** - vzdání se určitého příjmu a přenesení rizika na další subjekt (například pojišťovna).
- **Retence rizika** - přijetí všech rizik, kterým podnik čelí a nedělá s nimi vědomě nic.

Tyto čtyři možnosti, které jsou uvedeny výše, nejsou vzájemně výlučné. Někdy se může stát, že podnik může využívat přínosy z různých kombinací těchto možností. Záleží na konkrétní situaci v podniku. (20)

3.7.6.4 Mimořádné plány

Jsou předem sestavené postupy, kterými se bude projekt řídit v případě vzniku popsané rizikové události. **Havarijní plány** jsou předem připravené plány, které slouží ke zvládnutí

rizik s vysokými dopady na dosažení cílů projektu. **Mimořádné přirážky** jsou opatření v situaci, kdy vedoucí projektu či podniku snižuje míru rizika překročení nákladů nebo časového plánu projektu. (23)

3.8 Ekonomické zhodnocení

K posouzení ekonomického zhodnocení investice je vhodné vypočítat **čistou současnou hodnotu (NPV)**, která patří k nejběžnějším metodám posuzování. Obsahuje *peněžní toky (CF)*, *diskontní úrokovou míru (r)*, **jednotlivé roky (n)** a kapitálové výdaje, neboli *investiční náklady (IN)*. Dále zahrnuje celou dobu životnosti projektu. (39)

$$NPV = \sum_{n=0}^{t} \frac{CF}{(1+r)^n} - IN \tag{3.9}$$

Pokud má být investice realizována, čistá současná hodnota musí být kladné číslo. Pokud je vybíráno z více projektů, vybere se ten, který má nejvyšší hodnotu NPV. (39)

Další ukazatel popisuje výpočet **dobu návratnosti investic (TN_p)**, který se skládá z *investičních nákladů (IN)* a *peněžních toků (CF)*.

$$TN_p = \frac{IN}{CF} \tag{3.10}$$

Při použití ročních peněžních toků k výpočtu je výsledkem doba návratnosti jednorázové investice v letech. Čím více let má projekt dobu návratnosti, tím nižší je vypovídací hodnota tohoto ukazatele, protože neumí počítat s rozdílnými peněžními toky v jednotlivých letech a nezahrnuje diskont. (39)

Očekávaná peněžní hodnota (OPH) vypovídá o výhodnosti možné investice. Metodika výpočtu tohoto ukazatele je součin pravděpodobnosti (y) a výsledku (x). Výpočet má dvě větve výpočtu. Pravděpodobnost se skládá ze dvou částí, které dohromady dávají číslo jedna. Tato pravděpodobnost je rozdělena mezi dva faktory, existuje-li pravděpodobnost vzniku jevu jedna, je pravděpodobnost vzniku druhého jevu rovna rozdílu čísla jedna a pravděpodobnosti vzniku prvního jevu. Pak tedy existují i dvě hodnoty výsledků, s kterými jsou tyto pravděpodobnosti spjaty, jejich roznásobením vzniknou dvě očekávané hodnoty, které se sečtou a vznikne celková peněžní hodnota. (23)

$$OPH = (x_1 * y_1) + (x_2 * y_2) \tag{3.11}$$

Pokud je hodnota kladná, je vhodné do projektu investovat. Existuje-li více projektů, je to vhodná rozhodovací metoda, tzv. rozhodovací strom, kdy se vybere projekt s největší hodnotou, přičemž investice do všech projektů s kladným číslem je investicí přínosnou. (23)

4 Analýza problému

Druhá část této práce bude věnována praktické části, která nadále bude rozdělena do několika dalších částí obsahujících analýzy a metody identifikující slabiny v informačním systému a návrhy na jejich opatření.

4.1 Představení společnosti

Podnik, ve kterém jsou posuzovány vybrané faktory, vznikl v roce 1859 USA. Podnik se plošně zabývá hlavně výrobou kompresorů, dmychadel, pump, palivových systémů, dávkovacích čerpadel, centrálních stanic atd. Specializaci podnikání na trhu však pokrývá širší zaměření, nejen výrobní, ale např. částečně i oblast farmaceutického odvětví. Tato práce se ale zabývá posouzením stavu informačního systému pobočky mezinárodního podniku, která je umístěna v Brně v České republice od r. 2011 a zabývá se finanční stránkou podniku pro vybrané mezinárodní výrobní pobočky mateřského podniku. Existuje tu ještě i druhá, starší samostatná pobočka, která se ale zabývá distribucí dílů a ta nebude předmětem našeho zkoumání.

Zkoumaná finanční pobočka řeší finanční záležitosti pouze ve dvou vybraných zemích, a to v Anglii a Německu. Zahrnutí ostatních zemí do portfolia pobočky je součástí strategického a taktického plánování, kdy by se podnik měl rozrůst ze stávajících 50 zaměstnanců minimálně na dvojnásobek. Tento plán je plněn pouze z části, několik zemí čeká stále transfer do České republiky. Podpora hlavních činností je zabezpečena informačním systém SAP, na zpracování faktur se zde používá podpůrný software Brainware, který je propojený se systémem SAP.

Přestože podnik v Brně zaměstnává okolo 50 lidí, řadí se mezi malé nebo spíše střední podniky. Funguje na principu SSC[1]. SAP používaný v SSC se používá ve všech pobočkách amerického podniku, a proto při řešení nemá smysl zvažovat případnou změnu informačního systému.

Veškeré aktivity spojené s informačními technologiemi z oblasti instalace programů, nastavení PC, řešení IT problémů, zde doposud řeší externí IT podnik formou denních návštěv. Problematiku SAP a s tím související nastavení serverů, řešení problémů atd., obstarávají pracovníci podpory hlavně v Německu a v USA. Veškeré hardwarové vybavení podniku je zcela nové, výkonově přizpůsobené IS a ostatním softwarovým doplňkům.

[1]Shared service center – centrum sdílených služeb

U IS SAP se využívá vždy nejnovější verze, průběžně jsou prováděny update. I v Brně nedávno management podniku zaměstnal nového pracovníka na pozici SAP specialisty. SAP zde koresponduje s účetními standardy dle US GAAP. Jak bylo uvedeno, prozatím zde fungují finanční služby pouze pro dvě země, a to Anglii a Německo. Oddělení je rozděleno do dvou dílčích týmů. První z nich je **Accounts Payable** (AP), kde probíhají následující operace: zpracování přijatých faktur od dodavatelů, placení vzniklých závazků na základě domluvených platebních podmínek, automatické platby, manuální platby, telefonický styk s dodavatelem, evidence chybějících faktur, zasílání avíz atd. AP spolupracuje i s oddělením **Purchasing Department** (PD), které je umístěné vždy v mateřské zemi a realizuje objednávky zboží a služeb. Protože oddělelní PD často spolupracuje s dodavateli, mělo by být umístěné vždy blízko továrny (anglicky Plant), tedy v zemi, kde se daný produkt vyrábí. V obou případech Anglie i Německa se PD nachází v dané zemi. AP často komunikuje s PD, protože faktury jsou často zpracovávány na základě objednacího čísla.

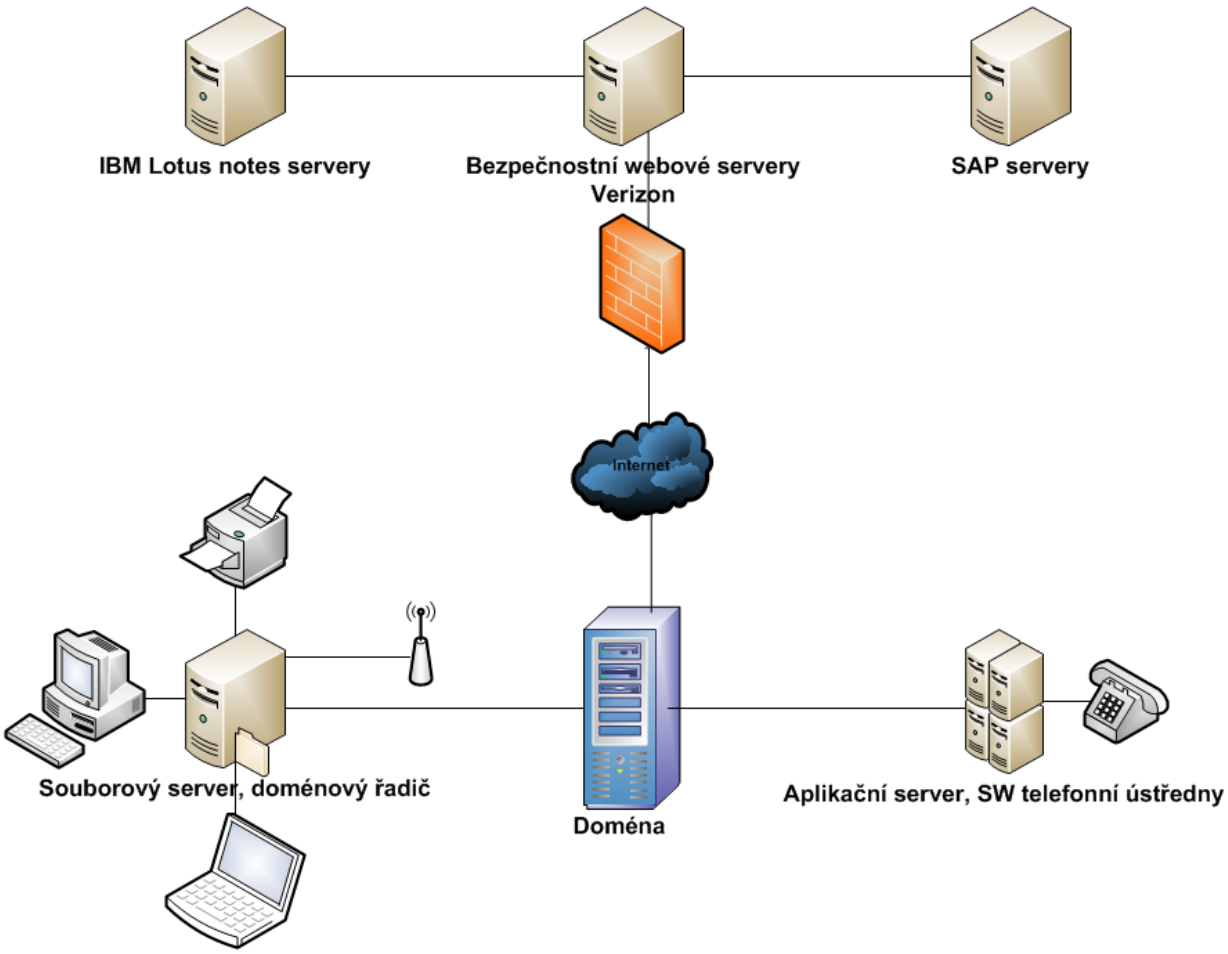
Druhé odvětví ve financích se nazývá **Accounts Receivable** (AR). Zde dochází na základě objednávky od odběratele k vystavení faktury, ta je zaslána odběrateli k uhrazení na základě domluvených platebních podmínek. Mezi další funkce patří přijímání plateb, jejich alokace, sledování nezaplacených faktur atd. Existuje ještě jedno odvětví, které patří do finančního oddělení s názvem **General Ledger** (GL), kde dochází k účtování transakcí na základě interních GL účtů dle US GAAP, avšak toto oddělení by mělo být přemístěno do České republiky v průběhu jednoho až dvou let.

4.2 Posouzení informačního systému

Posouzení informačního systému vychází ze zpracovaných dotazníků uvedených v příloze A.1.1. Výsledky vyplněných dotazníků jsou následně porovnány s výsledky dotazníků vyplňovaných v jiných podnicích, které jsou svým zaměřením a velikostí podobné analyzovanému podniku.

4.2.1 Architektura podnikové sítě

Architektura podnikové sítě je propojena tunelem se servery umístěnými v Německu přes bezpečnostní servery s bezpečnostním software Verizon, který obsahuje firewall proti vnějším útokům. Přes tento server jsou propojeny SAP servery umístěné v USA a IBM Lotus Notes servery v Německu.



Obrázek 4.1: Architektura podnikové sítě

Internet tedy prochází přes německé bezpečnostní servery obsahující Verizon. V Brně je umístěna lokální doména aplikačního serveru obsahujícího software telefonní ústředny, přes kterou jsou propojeny telefonní linky umístěné u každého počítače. Dále jsou připojeny souborový server a doménový řadič s počítači, notebooky a periferiemi. Podniková síť v Brně je propojena sítí 1Gb LAN, v podniku se využívá i bezdrátové sítě wifi pomocí routeru, kde je přístup chráněn šifrováním WPA2. Připojení k internetu je řešeno přes tunel v Německu ADSL synchronním připojením, disponující rychlostí 4 Mb/s download a 4 Mb/s upload.

4.2.2 Efektivita informačního systému

Jak bylo uvedeno, podnik zaměstnává okolo 50 zaměstnanců různé národnosti včetně managementu, hlavním předmětem podnikání je zajišťování finanční činnosti.

Dotazník vyplnilo 23 zaměstnanců pracujících se systémem SAP., většina používá podpůrnou aplikace Brainware, všichni pak pracují s kancelářským software Microsoft Office.

4.2.2.1 Řešení informačního systému SAP

Většina z dotazovaných, jak je uvedeno v příloze A.1.1 nezná stáří IS SAP. IS je neustále aktualizován posledními verzemi, aktuálnost je tedy na velmi dobré úrovni. Silné stránky IS SAP jsou především přesnost a úplnost dat poskytovaných systémem, rychlost odezvy/zpracování a mělo by být i programové vybavení, které, jak se ukazuje, je snad jediným slabším místem, konkrétně podpůrná aplikace Brainware, tedy software na zpracování skenovaných faktur. Problém této části spočívá v rychlosti odezvy tohoto programu, což je způsobeno serverem umístěným až v USA. Snaha o řešení problému vyšla prozatím naprázdno.

Za slabé stránky posuzovaného systému je považována neuspokojivá uživatelská přívětivost. SAP je z uživatelského hlediska složitější na ovládání všech transakcí např. ve srovnání s IS Oracle, kde na provedení určitého procesu stačí jedna činnost, v SAPU jsou nutné třeba dvě nebo tři činnosti[2]. Při porovnání odpovědí v jiných podnicích jsou odpovědi téměř podobné a nijak závratně se neliší.

4.2.2.2 Zaměstnanci podniku

V podniku pracuje poměrně mladý kolektiv s průměrným věkem do 30 let, což je výhodou při plánování různých aktivit nebo teambuildingů. Standardem je tu minimálně vzdělání na úrovni Bc., což je rozdíl oproti dřívější době. Odpovědi na stejné otázky dopadly u ostatních podniků podobně.

Z vyplněných dotazníků lze vysledovat jeden aspekt, který poukazuje na problém s délkou zaměstnanosti pracovníků v podniku, kdy v Brně jsou zaměstnanci v pracovním poměru kratší dobu než v ostatních sledovaných podnicích. Při nedávném anonymním šetření spokojenosti pracovníků byla však zjištěna i v tomto bodě spokojenost, mírný nedostatek

[2]Osobní zkušenost autora

pociťovali někteří v chybějících „sick days“ [3]. Ostatních benefitů podnik nabízí spoustu – stravenky, flexipasy, týden dovolené navíc. Podpora vzdělávání pracovníků je také na slušné úrovni, podobně jako u ostatních dotazovaných podniků.

Jak bylo uvedeno v průzkumu, všichni pracovníci používají ke své práci informační systém na denní bázi, což podtrhuje významnost a závislost na informačním systému SAP. Převážná část uživatelů k IS/IT má kladný vztah, všichni jsou počítačově gramotní, bez toho si lze kvalitní působení zaměstnance v podniku těžko představit.

4.2.2.3 Úroveň podpory

Spokojenost pracovníků s celkovou úrovní podpory při práci s informačními systémy je stejná jako u pracovníků ostatních srovnávaných podniků. Podporu v podniku zajišťuje externí IT podnik, tato část procesu je tedy outsourcována. Podpora IS SAP je vedena v Německu. Podpora procesů v SAP se nedávno znatelně zvýšila náborem specialisty na procesy v SAP. Pokud se jedná o běžné uživatelské problémy jako např. složitější instalace software, zapojení PC, běžná denní údržba apod., tyto záležitosti řeší přímo pracovníci v podniku. V podniku ale neexistuje zodpovědná IT osoba.

Úroveň technické podpory je na dobré úrovni, externí IT podnik dokáže vyřešit problém do jednoho dne. Je na škodu věci, že podpora je poskytována pouze v dopoledních hodinách pracovního týdne, pak už existuje jen podpora na telefonu, tzv. hot-line. V případě nutnosti instalace programů je požadavek splněn většinou rychle. Každý uživatel má i možnost instalovat na svůj PC jakýkoliv program, což je na jedné straně výhoda, na druhé straně ale větší nevýhoda z důvodu možnosti ovlivnění funkce systému případnou chybou instalace, tedy vznikem nějakého incidentu a je tento přístup i možným rizikem pro podnik.

4.2.2.4 Úroveň řízení

V podniku neexistuje osoba, která by byla zodpovědná za řízení informačních systémů. Předmětem IS není pouze software jako prostředek k vykonávání procesů, ale zahrnuje i jeho okolí a jakýkoliv incident může ohrozit práci s IS. Pokud v podniku neexistuje CIO, je obtížné dořešit případnou ztrátu, která může špatnou činností někoho ze zaměstnanců vzniknout.

Podniková strategie je zaměstnancům prezentována v nepravidelných intervalech. Většinou to bývá u nějakých příležitostí podniku, tedy podobně jako u ostatních dotazovaných podniků. Ale i tak informovanost pracovníků o přínosu plnění podnikových cílů v této pobočce ale předčila ostatní dotazované podniky o 24 %. Tento výsledek může poukazovat na dobré řízení posuzovaného podniku.

Dodržování pravidel pro práci s IS je na stejné úrovni jako v ostatních dotazovaných podnicích. Odpověď zněla, že existují pravidla, ale nejsou příliš kontrolována nebo vyžadována, což je další chyba IS, která by měla být napravena, jinak může vzniknout například

[3] Nezbytná doba na léčení chřipkového onemocnění, bývá udělováno zpravidla 2-3 dny na celý rok, které si může zaměstnanec vybrat v případě intenzívního léčení přicházejícího krátkodobého chřipkového onemocnění, místo dlouhodobého, bez nutnosti doložení lékařského potvrzení.

bezpečnostní incident.

4.2.2.5 Efektivnost informačního systému

Pracovníci vnímají nasazení IS jako nezbytnost pro jejich práci v podniku, podobně jako v jiných podnicích, což lze jen potvrdit, neboť bez kvalitního IS bychom si mohli těžko představit odpovídající fungování posuzovaného podniku.

Okolo 82 % pracovníků z průzkumu si myslí, že by jim informační systém mohl více pomáhat v jejich práci, což je o 6 % více, než u pracovníků srovnávaných podniků. To může indikovat nižší efektivnost posuzovaného informačního systému. Je to způsobené až někdy přílišnou složitostí IS SAP. Aby člověk mohl normálně pracovat s IS, musí k tomu znát spoustu různých transakcí a provádět více než jeden krok k uskutečnění jedné operace s fakturou. Tuto situaci nelze snad ani kvalifikovat jako velký problém, souvisí totižse schopnostmi a znalostmi každého zaměstnance.

Školení zaměstnanců v posuzovaném podniku je na dobré úrovni. Své pracovníky školí jak jejich nadřízení, tak i specialisté na SAP. Běžnou praxí je zaškolení nově příchozího služebně starším kolegou, který už procesy dokonale zná. 91 % zaměstnanců se účastnilo školení na SAP, což je více jak u srovnávaných podniků. 90 % z nich uvedlo, že pro ně školení mělo přínos, u ostatních podniků to bylo 89 %, přičemž 78 % má zájem o školení na IS, to je také více než u srovnávaných podniků.

4.2.2.6 Bezpečnost informačního systému

Výsledky této podkapitoly jsou negativní. Posuzovaný podnik **nemá** žádnou **bezpečnostní politiku**, obecná pravidla, která by měla být striktně vymáhána a dodržována, nejsou známa. Zvyšuje to riziko zneužití dat a ohrožení práce s IS. Úroveň bezpečnostní politiky je u posuzovaného podniku rozhodně na nižší úrovni, než u srovnatelných podniků. Po vyhodnocení dotazníků byli někteří zaměstnanci dotázáni, co si představují pod pojmem bezpečnostní politika informačního systému, nikdo však nebyl schopen tento termín řádně definovat. Následující výčet možných aktivit ukazuje slabiny, které by bezpečnostní politika měla podchytit a řešit:

Nekontrolovatelné připojování různých zařízení do systému. Do počítačové sítě si pracovníci mohou připojovat vlastní soukromá zařízení, což je z dalších možných bezpečnostních rizik. Připojování soukromých zařízení do podnikové počítačové sítě lze i jinými osobami než zaměstnanci, dle vyhodnocení dotazníků riziko v této oblasti je u posuzovaného podniku nižší než u srovnatelných podniků. Pokud jsou ignorovány odpovědi „nevím“, jsou pak obě vyhodnocení srovnatelná. Možnost připojovat přenosná paměťová média zaměstnanci k jejich počítači a tedy i (možné) riziko zneužití dat podniku v této oblasti je u posuzovaného podniku stejné jako u srovnatelných podniků.

Nezálohování dat. 8 % pracovníků nemá vůbec řešenou zálohu dat na PC. Tento nedostatek by měl být v rámci kompetence bezpečnostní politiky co nejdříve napraven.

Ztráta dat není otázkou zda, ale kdy. Zálohování dat uložených na počítačích a riziko z této oblasti plynoucí je u posuzovaného podniku stejné jako u srovnatelných podniků. Množství ztracené práce při havárii počítačů pracovníků je údajně téměř nulové, většina dat je mimo zaměstnancův počítač. To se ale netýká samozřejmě vlastních souborů uložených na ploše a ve složkách.

Neznalost důležitosti ochrany bezpečnosti dat. 34 % pracovníků má kritické neznalosti v oblasti bezpečnosti dat na jejich počítačích. Neuvědomují si, že ochrana přihlašovacím jménem a heslem do počítače nechrání data na něm, pokud je disk vymontován z počítače. Je doporučeno lepší zabezpečení v této oblasti, hrozí ztráta podnikových dat především u notebooků. Riziko zneužití dat v této oblasti je u posuzovaného podniku stejné jako u srovnatelných podniků.

Nedodržování postupů pro bezpečné přihlašování do systému. 17 % procent pracovníků nebere ochranu svých přístupových hesel do systému příliš vážně. To může vést k nižší bezpečnosti dat. Úroveň ochrany hesel je dobrá. Riziko prozrazení přístupových hesel pracovníků je u posuzovaného podniku stejné jako u srovnatelných podniků.

Nekontrolovatelný přístup na internet. 4 % pracovníků chybně reaguje na možné ohrožení bezpečnosti jejich počítače z internetu. Vhodné by bylo proškolení pracovníků. 91 % pracovníků má přístup na internet (s omezením na stránky s násilím a pornografií). Pokud tito pracovníci nepotřebují internet pro svou práci, může jít o zbytečné zvýšení bezpečnostního rizika a možné snížení produktivity práce. Riziko v této oblasti je u posuzovaného podniku stejné jako u srovnatelných podniků.

Ohrožení podniku instalací nelegálního software. V podniku existuje možnost instalovat programy přímo zaměstnanci na jejich počítače a existuje tedy i riziko trestně právní odpovědnosti za instalaci či využívání nelegálního software a ohrožení bezpečnosti informačního systému, riziko v éto oblasti je u posuzovaného podniku vyšší než u srovnatelných podniků.

4.2.2.7 Informační systém jako služba – outsourcing

Účastníci byli tázáni na přínos informačního systému, zda jej chápou jako službu, podpůrný proces své práce nebo jako integrální součást svých procesů. Tyto odpovědi pak mohou pomoci s úvahami o možném outsourcingu informačního systému nebo jen jeho části.

Většina zaměstnanců neví, jak má IS SAP vnímat, v odpovědích převažoval spíše názor vnímání IS SAP jako interní služby. Všichni zaměstnanci, kteří mají zkušenosti s outsourcingem nebo externím zajištěním nějaké služby v posuzovaném podniku, odpovědělo, že mají s outsourcingem pozitivní zkušenost. Při porovnání odpovědí u ostatních podniků lze

konstatovat, že v těchto podnicích má 71 % pracovníkůpozitivní zkušenosti s outsourcingem nebo externím zajištěním nějaké služby.

Tato podkapitola se zabývá využívání externích služeb, tzv. outsourcingu. Dotazovaní byly tázání za účelem zjištění, jestli pracovníci chápou informační systém jako službu, podpůrný proces své práce nebo jako integrální součást svých procesů. Tyto odpovědi pak mohou pomoci s úvahami o možném outsourcingu informačního systému nebo jen jeho části.

Většina zaměstnanců neví, jak má SAP vnímat jako externí službu, jinak spíše převažuje názor, že SAP nevnímají jako externí službu. Všichni zaměstnanci, kteří mají zkušenosti s outsourcingem nebo externím zajištěním nějaké služby v posuzovaném podniku, odpovědělo, že mají s outsourcingem pozitivní zkušenost. S porovnáním ostatních firem, tak tam výsledky říkají, že 71 % pracovníků má pozitivní zkušenosti s outsourcingem nebo externím zajištěním nějaké služby.

4.2.3 Ohodnocení jednotlivých částí informačního systému

Tato podkapitola se opírá o výsledky z dotazníku, uvedené v kapitole A.1.2, vyplněného řídícím pracovníkem v podniku. Toto hodnocení se nazývá HOS 8, protože porovnává 8 klíčových oblastí informačního systému. Mezi tyto klíčové oblasti patří hardware, software, orgware, peopleware, dataware, zákazníci, dodavatelé a management IS.

4.2.3.1 Hardware

I když je hardware poměrně nový, výsledky poukazují na některé nevyhovující výkonové potřeby systému, tzn. ukazuje na nutnost inovace či posílení této oblasti. Jak bylo uvedeno, hardwarové vybavení v posuzovaném podniku je na velmi dobré úrovni, bylo instalováno před cca 1,5 rokem. Jediný, již zmíněný problém, je rychlost odezvy serveru, což je dáno pravděpodobně především vzdáleností jeho umístění až v USA. Problém se i přes veškeré snahy nepodařilo dosud vyřešit. Pokud tedy byla prověřena rychlost počítačové sítě, měla by se zkontrolovat i kvalita počítačových sítí.

Připojení k síti je zajištěno pomocí 1Gb LAN, servery umístěné v jiných zemích ovlivnit podnik nemůže, proto je zřejmé, že výsledky dotazníku poukazují na doporučení obnovy techniky. Každý zaměstnanec má stolní počítač se dvěma monitory značky Acer nebo Samsung. Pracovníci managementu používají notebook. Jak PC tak notebooky jsou navzájem hardwarově kompatibilní.

Hardware PC:

Základní deska:	Dell Inc.
Procesor:	Intel Core i5 2500 @ 3,30GHz
Paměť:	4,00 GB Dual-Channel DDR3 @ 1333 MHz
Disk:	250 GB Seagate ST3250312AS (SATA
Grafická karta:	Intel(R) HD Graphics Family
DVD mechanika:	TSSTcorp DVD+-RW TS-H653H
Audio:	Realtek High Definition Audio

Hardware notebooků:

Základní deska:	Dell Inc.
Procesor:	Intel Core i5 2540M @ 3,30GHz
Paměť:	4,00 GB DDR3 @ 1333 Mhz
Disk:	Western blue edition 250GB 5400 ot.
Grafická karta:	Intel HD Graphics 3000
DVD mechanika:	Optická mechanika DVD-RW
Audio:	Realtek High Definition Audio

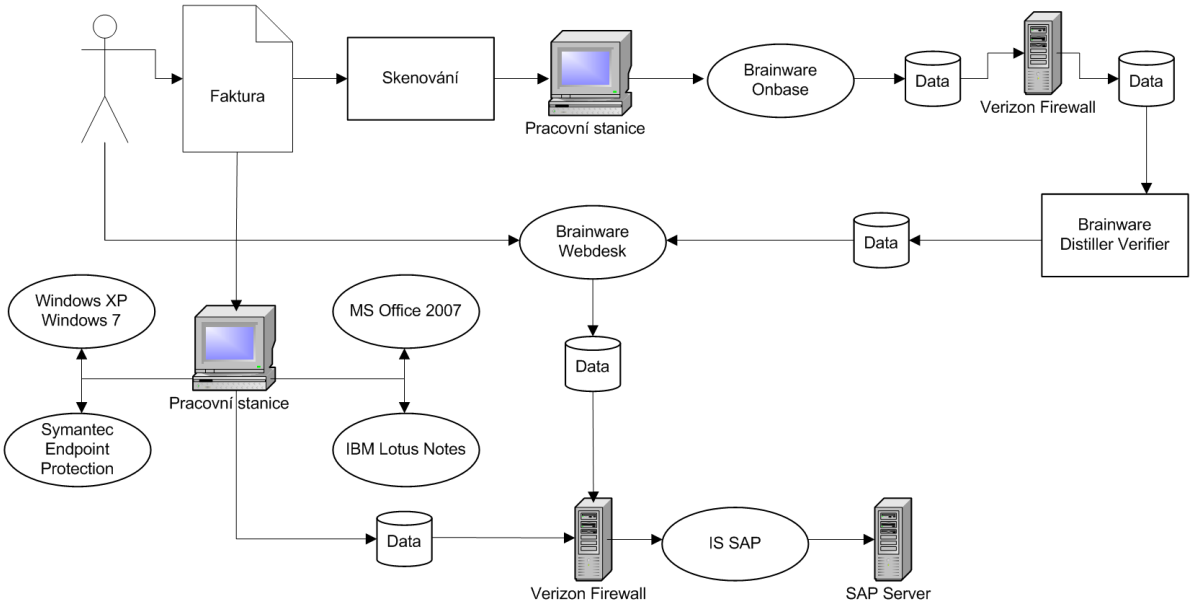
Výše uvedené sestavy zajisté uspokojí veškeré požadavky na plynulou práci s informačním systémem a ostatními aplikacemi. Mezi další hardware náleží i výstupní zařízení či periferie jako např. tiskárny. Používají se černobílé laserové tiskárny značky Kyocera, dále pak barevné tiskárny značky OKI, umožňující skenování a faxování.

4.2.3.2 Software

Při výběru informačního systému je třeba předem stanovit, které funkce jsou požadovány. Posuzovaný systém neobsahuje všechny důležité funkce potřebné pro jeho uživatele. SAP umí zpracovávat pouze již schválené faktury Dříve k tomu byli potřeba minimálně dva lidé, jeden schvalující, další pak účtující. Tento krok byl zkrácen pomocí podpůrné aplikace Brainware, propojené se SAP, která je určená pro zpracování všech faktur. K řádnému využití je však třeba doplnit systém ještě o aplikace Onbase, Distiller Verifier a Webdesk. Faktura naskenovaná do aplikace Onbase je odeslána do aplikace Distiller Verifier, kde je nutný zásah pracovníka, který opraví chyby a fakturu odešle do aplikace Webdesk. Po schválení putuje rovnou do systému SAP. Existuje však ještě jeden druh atypických faktur s objednacím číslem, kdy pouze stačí zásah zaměstnance, který upraví linky na objednacím čísle, tak jak je to na faktuře a vytvořeno v systému. Tato faktura pak putuje také do IS SAP. Z hlediska problémů odezvy a výpadku serveru se krok pro zpracování faktur s objednacím číslem musel zrušit a tato aplikace se využívá pouze pro schvalování faktur, protože je audit lehce dohledá. Z uvedených důvodů je patrné, že Brainware je nevyhovující aplikací a bylo by vhodné nalézt přijatelné řešení k odstranění jeho nedostatků. Mezi další softwarové produkty patří Microsoft Office 2007, který je nezbytný pro práci každého

zaměstnance. Operační systém se využívá převážně Windows XP, dále pak již i Windows 7 Antivirovou ochranu zajišťuje Symantec. Podnik využívá vnitropodnikového intranetu k odběru novinek adresovaných z mateřské společnosti, k vyhledávání kontaktů, k vývoji akcií apod. Jako e-mailový klient a komunikaci přes intranet síť slouží program Lotus Notes od firmy IBM. Software Verizon slouží jako ochranný prvek serverů proti vnějším útokům, software včetně hardware je umístěn v Německu, nelze tedy jakoukoliv změnu ovlivnit. Za zmínku stojí ještě software telefonní ústředny, bez kterého nelze provozovat telefonní linky, přestože je tento software bezpečný a v případě problému stačí restartovat aplikační server.

Závěrem lze tedy konstatovat, že efektivita práce s informačním systémem se nejeví příliš jako vyhovující, neboť systém SAP je poněkud složitější na ovládání (uživatel musí provést více transakcí k tomu, aby dosáhl požadované činnosti IS), nevyhovující se jeví způsob prezentace chybových hlášení IS SAP, uživatelé nemají přehled o významu chybových hlášení. Komunikační prostředí systému by mělo být jednotné, jasné s přehledným a uživatelsky přátelským stylem. Z uvedených důvodů by bylo tedy vhodné provést odpovídající opatření ke zvýšení spokojenosti uživatelů IS.



Obrázek 4.2: Proces navazujících programů IS

4.2.3.3 Orgware

V podniku neexistují definované postupy a směrnice pro řešení havarijních stavů systému. Pokud neexistují žádné pracovní postupy nebo předpisy, pak existuje bezpečnostní chaos v podniku, může dojít k výrazné ztrátě a ohrožení fungování IS. Firma by měla mít stanovena přísná bezpečnostní pravidla, pravidelně je aktualizovat, seznámit a proškolit jimi každého zaměstnance, příp. i opakovaně po každé aktualizaci, proškolení pak stvrdit podpisem každého zaměstnance.

Bez pravidel a provozu bezpečnosti informačního systému lze IS SAP považovat za ne zcela efektivní s možností vzniku ohrožení podniku nefunkčností systému.

4.2.3.4 Peopleware

S předchozím bodem souvisí potřeba školení pracovníků na práci s informačním systémem SAP a s pravidly bezpečnosti. Zatímco uživatelská školení na IS probíhají, v pravidlech bezpečnosti nikoliv. Bylo by vhodné tedy zvážit, jak dalece zvýšit podporu dalšího celkového vzdělávání pracovníků, popřípadě jak tato vzdělávání zlepšit a pokud ano, jakou formou. Jednoznačně je třeba provést opatření ve vzdělanosti v oblasti bezpečnosti po všech stránkách.

Chybí možná i listinná forma pravidel, kde by byla uvedena zastupitelnost klíčových pracovníků při práci s IS. Bylo by vhodné zvýšit důraz na dodržování těchto pravidel s vyvozením důsledků při jejich porušování.

4.2.3.5 Dataware

Pracovníci nemají jasně vymezenou odpovědnost za data, která spravují. Opět částečně souvisí s bezpečnostní politikou, hlavně s podnikovými procesy IS. Mělo by být jasně vymezeno, kdo a kdy musí data vložit do IS. Tato podmínka je splněná nyní pouze částečně. Vymezení existuje pouze slovně, nikoliv nějakým písemným příkazem či jiným dokumentem. A to může být problém u bezpečnostního auditu. Chybí tu tedy SOD[4], který by tento problém mohl vyřešit.

Ne všichni zaměstnanci mají ke své práci všechny informace, tento problém se ale postupně řeší. Je to způsobeno jednak neustále novými projekty, stabilizací procesů atd. Cílem tedy je vytvoření jednotného dokumentu s podchycením všech procesů. Je logické, že tento dokument se bude lišit podle jednotlivých týmů, důležité je zajistit, aby pracovníci nedostávali nepřesná a nadbytečná data.

V podniku neprobíhá pravidelné zálohování dat na počítačích uživatelů, což některým může způsobit vážné problémy, dojde-li k bezpečnostnímu incidentu. Měly by existovat i plány obnovy dat ze záloh v případě havárie systému. Média se zálohami by měla být označena a dobře chráněna proti zneužití a poškození.

4.2.3.6 Zákazníci

Uživatel je zde chápán z pohledu zákazníka. Veškeré cíle IS by měly být definovány vzhledem k jejich zákazníkům. Měly by být definovány metriky informačního systému vzhledem k jeho zákazníkům (uživatelům) - tedy ukazatele, kterými se měří plnění role informačního systému vůči zákazníkům, jaká je s ním spokojenost atd., což by pak mělo být pravidelně vyhodnocováno. Pokud v podniku neexistuje CIO, lze jen těžko o něčem

[4]Segregation Of Duties - rozdělení pravomocí (písemně), jinými slovy interní kontrola nad vnitropodnikovými procesy, například jeden člověk nemůže zároveň schválit, zaúčtovat a zaplatit fakturu, je to rozděleno mezi několik osob, aby bylo zabráněno podvodům.

podobném prozatím uvažovat. Podnik by se měl více soustředit na zkoumání přínosů informačního systému zákazníkům. Výstupy z IS by měly být dobře upraveny na míru zákazníkovi. Rychlost odezvy samotného systému SAP je na velmi dobré úrovni. Chybí však ochrana citlivých obchodních dat o zákaznících.

Lotus Notes je možné propojit i s mobilními zařízeními, jako je iPhone od firmy Apple a Blackberry od firmy RIM. Toto je alternativní cesta přístupu k informacím, avšak tuto možnost má pouze management. Ještě jednou je nutné upozornit na aspekt nemožnosti měnit informační systém nebo jiné programy. Všechny pobočky používají SAP s modulem Brainware a Lotus Notes.

4.2.3.7 Dodavatelé

IT podpora v podniku je zde chápána z pohledu dodavatelů. Pokud zde neexistuje CIO, tuto funkci plní externí IT podnik.

V podniku není vůbec využíváno SLA s dodavatelem IS, přestože nezajišťuje přímo procesy ohledně IS procesů. Tento nedostatek supluje především podpora SAP přímo z Německa. V případě, že by externí IT podnik neplnil některé z požadavků, jak by bylo uvedeno ve smlouvě, není možné uplatnit nějaké sankce.

Bylo by vhodné zlepšit technickou a uživatelskou podporu. Zdá se totiž, že dodavatel IS nejeví zvláštní zájem o svého zákazníka a neposkytuje tedy odpovídající služby v požadované oblasti.

4.2.3.8 Management IS

Manažeři musí trvat na dodržování všech existujících nebo budoucích pravidel provozu a bezpečnosti informačního systému a kontrolovat jejich dodržování. Měli by poskytovat dodavateli IS zpětnou vazbu ohledně spokojenosti a nových námětů na zlepšení. Zpětná vazba se dosud v podniku neposkytuje, řeší se pouze případné stížnosti.

Pokud podnik nemá informační strategii, pak lze jen těžko zkoumat efektivnost takového systému. Z toho všeho pak může plynout situace, kdy si management dostatečně neuvědomuje potenciál a význam IS pro činnost a rozvoj podniku.

Hlavní problém tohoto podniku je, že zde neexistuje hlavní manažer informačních systémů, tzv. CIO. Rozvoj a zabezpečení informačních systémů jsou zde vystaveny vysokému riziku zneužití nebo poškození.

Srovnání stavu informačního systému

Jak je uvedeno v tabulce A.1 v příloze A.1.2, nejvíce utrpělo hodnocení oblastí orgware, dodavatelé a management IS. Tyto oblasti byly ohodnoceny úrovní 2 z možných 4. Ostatní oblasti byly ohodnoceny úrovní 3. Proto by bylo vhodné se popřípadě zaměřit na oblasti, které byly ohodnoceny jako spíše špatná úroveň, tedy známkou 2.

I úroveň HOS byla porovnána s ostatními podniky o celkovém počtu 282 (graf na obrázku A.3). Průměrná úroveň oblastí HOS ostatních podnikům se pohybuje okolo 3 bodů, cože je lepší jak u posuzovaného podniku.

Jelikož některé posuzované oblasti HOS jsou na úrovni 2, ostatní oblasti jsou tím limitovány také, takže lze říci, že úroveň oblastí HOS je na úrovni 2 (graf na obrázku A.2). Proč tomu tak je? Například pokud si koupíte špičkovou zvukovou kartu za 10000 Kč do počítače, k tomu si ale dokoupíte reprosoustavu za 500 Kč, tak asi budete těžko poslouchat kvalitní reprodukovaný zvuk, protože je právě limitován lacinou reprosoustavou.

4.2.4 Shrnutí a stanovení problému

První částí posouzení efektivnosti IS vyšlo najevo, že hlavní problémy spočívají v podpůrné aplikaci IS SAP, která se nazývá Brainware a v chybějící bezpečnostní politice. Chybějící bezpečnostní politika v podniku se jeví jako více závažnější. V druhé části bylo posouzeno 8 klíčových oblastí IS, kde se jako problémové jeví tři oblasti, a to orgware, dodavatelé a management IS. Všechny tyto oblasti jsou úzce spojeny s **chybějící bezpečnostní politikou**. Z toho lze tedy usuzovat,na problém, na který je nutné se v následujících částech práce zaměřit. Ostatní nedostatky IS mohou pak být řešeny v kapitole návrhu vlastních řešení, ale jen okrajově jako součást zavádění bezpečnostní politiky v podniku.

4.3 Analýza vnitřního a vnějšího prostředí

V této podkapitole bude provedena analýza PEST vnějšího prostředí podniku, pak vnitřního prostředí rozborem 7S faktorů a nakonec bude aplikována metoda kombinující analýzu vnitřního i vnějšího prostředí, SWOT analýza, která pomůže identifikovat i strategie.

4.3.1 PEST analýza

Analýza vnějšího prostředí podniku zahrnuje politicko-právní, ekonomické, společenské (sociální), technické (technicko – technologické) faktory.

4.3.1.1 Politicko - právní faktory

Dotace na vytvoření nových pracovních míst. Dotace na vytvoření nových pracovních míst. Tento faktor má pozitivní vliv na podnik z hlediska získání dalších peněžních prostředků na fungování podniku. Zkoumaný podnik zaměstnává dosud okolo 50 zaměstnanců, v dalším období se bude pravděpodobně rozrůstat. K naplnění tohoto plánu má podnik právo zažádat o dotaci na vytvoření nových míst, což je velmi dobrá příležitost k pokrytí částečných nákladů k rozšíření činnosti podniku na českém trhu.

Zákon č. 435/2004 Sb. (31) upravuje detaily této problematiky. Výše dotace může dosahovat až 80 000 Kč připadající na jedno nové pracovní místo, v závislosti na předpokládaných nákladech s jeho vytvořením. Této dotace lze využívat maximálně po dobu 24 měsíců. Dotaci nelze přiznat zpětně, pokud podnik tedy nezažádal o dotace před zřízením pracovních míst, může tak učinit nyní před zřízením dalších pracovních míst, která jsou plánována.

Daň z přidané hodnoty. Dalším důležitým faktorem je daň z přidané hodnoty DPH, která je posuzována ze dvou pohledů, a to mezinárodního a národního. Z hlediska národního sazba DPH od ledna 2012 vzrostla postupně ze snížené sazby DPH z 10 % na 14 %, v roce 2013 pak na 15 %, seznam položek se nijak výrazně nezměnil. Základní sazba DPH zůstala v roce 2012 na 20 %, od ledna 2013 se zvýšila na 21 %. Posuzovaný podnik tento faktor může ovlivnit nákupem materiálů a služeb z podniků umístěných v České republice.

Z hlediska mezinárodního, v Anglii, sazba DPH vzrostla v roce 2011 ze 17,5 % na 20 %, snížená sazba činí 5 %. Tyto změny mohou ovlivnit obchody v rámci ostatních podniků zabývajících se výrobou komponent určené pro další prodej. Měny daňových sazeb by neměly výrazně ohrozit byznys posuzovaného podniku. Je vhodné věnovat pozornost vývoji DPH v Anglii a Německu, v případě neúměrně vysokých daní se může výrazně snížit objem uskutečněných obchodů, to může následně vést k poklesu objemu výroby a prodeje produtků podniku, což by mohlo výrazně negativně ovlivnit existenci pobočky v České republice.

Za poslední 3 roky v mnoha zemích Evropské unie došlo ke zvyšování DPH z důvodu nastupující krize šířící se napříč celou Evropskou unií. Tento trend, zvyšování sazeb DPH,

se ale Německa netýká. Základní sazba DPH je v Německu 19 %, snížená 7 %, což je v porovnání s ostatními zeměmi EU průměrná sazba.

Z hlediska informačního systému velmi záleží na vložení správných daňových sazeb při účtování přijatých nebo vydaných faktur, jinak hrozí sankce ze strany finančního úřadu.

Regulace v oblasti zahraničního obchodu. Důležitým faktorem je i clo. Podnik z podstatné části nakupuje a prodává v rámci Anglie a Německa, pokud ne v rámci dané země, tak v rámci Evropské unie, v tomto případě se clo podniku netýká. V případě obchodování mezi zeměmi Evropské unie se nejedná o dovoz nebo vývoz, ale funguje zde jednotný vnitřní trh, tedy volný pohyb zboží. Dodávky se neproclívají, pro výrobky nebo služby platí jednotné normy.

Neexistují ani žádné technické, hygienické nebo veterinární bariéry. Embargo nebo kvóty jsou z posuzovaného pohledu zanedbatelné.

Pracovní právo. Pracovní právo řeší Zákon č. 262/2006 Sb. (25), tedy zákoník práce, který upravuje právní vztahy mezi zaměstnanci a zaměstnavateli. Je založen na uzavření smlouvy mezi zaměstnancem a zaměstnavatelem. Ze zákona existuje určitá zkušební doba, na základě které může být se zaměstnancem i bezdůvodně ukončen pracovní poměr, stejně tak tomu může být i ze strany zaměstnance. Tato doba je 3 měsíce, u zaměstnanců pracujících na vedoucí pozici (managementu) může tato doba být prosloužena na 6 měsíců. Další detaily ohledně pracovního práva jsou uvedeny v zákoníku práce.

Z odborného pohledu je vhodné zvážit, jestli mezi zaměstnanci a zaměstnavatelem vzniká klasický pracovní poměr bez existence či na základě existence kolektivní pracovní smlouvy. Z toho je patrné pak, zda v podniku pracují odbory, což může v podniku zcela změnit situaci mezi zaměstnanci, zaměstnavatelem a stavem pracovních podmínek. V posuzovaném podniku zatím žádné odbory neexistují.

Legislativa upravující bezpečnostní politiku. Z legislativního hlediska upravuje bezpečnostní politiku zákon č.412/2005 Sb. (26), o ochraně utajovaných informací a bezpečnostní způsobilosti. Tento zákon upravuje podmínky pro stanovení informací jako informací utajovaných, možnosti přístupu k nim, včetně dalších požadavků na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy.

Bezpečnostní politika IS je dokonce i upravována vyhláškou č. 523/2005 Sb. (30) o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení a o certifikaci stínících komor. Vychází z vyhlášky č. 56/1999 Sb., o zajištění bezpečnosti informačních systémů nakládajících s utajovanými skutečnostmi, provádění jejich certifikace a náležitostech certifikátů, byla novelizována 1.1.2006.

4.3.1.2 Ekonomické faktory

Nezaměstnanost. Nezaměstnanost tento podnik určitě svým způsobem ovlivní. Pokud bude na trhu práce existovat vysoká míra nezaměstnanosti, tak většina lidí bude doma na

podpoře, z čehož vyplývá, že budou nuceni šetřit, jinak nebudou mít žádné prostředky, za které by si pořídili výrobky či služby. Existují názory, že vysoká míra nezaměstnanosti posuzovaný podnik neovlivní, nicméně se lze domnívat, že tomu může být právě naopak. K tomuto přesvědčení mě vede již uvedené směřování koncového výrobního řetězce ke spotřebiteli. Pokud spotřebitel nenakupuje, poslední článek výrobního řetězce nemá co prodávat, a tak neobjednává materiál určený k výrobě. Podniky pak krachují. Nezaměstnanost v České republice překročila 10 % (29) na začátku roku 2013, což je nejvíce od dob rozdělení Československa. Je ovšem pravděpodobné, že se tohle číslo zlepší nejpozději na přelomu jara a léta, kdy začnou sezónní práce.

Průměrná mzda. Může ovlivnit poskytování služeb ve finančním sektoru pro výrobní podnik, myšleno především z pohledu mezinárodního. Dle Českého statistického úřadu 3.čtvrtletí roku 2012 byla průměrná mzda 24 514 Kč (28). Pro porovnání ve Velké Británii je průměrná měsíční mzda 60 000 Kč, v Německu 91 600 Kč. Samozřejmě každé srovnání selhává, neboť nelze vytrhnout jen jeden údaj z komplexu, tedy z vlastního prostředí daného státu. Ke srovnání by bylo nutné vzít v úvahu i ceny služeb, potravin, jiných výrobků, energií apod.I když prozatím je cena práce z hlediska investorů výhodnější v České republice, lze nalézt lokality, kde je situace ještě výhodnější Znamená to hrozbu přemístění finanční pobočky z ČR do jiné země s lepší finanční atraktivitou pro případné investory podniku.

Inflace. V roce 2013 je průměrná míra inflace v České republice 3,2 % (28). Pokud v roce 2012 existoval spotřební koš v hodnotě 10 000 Kč, tak v roce 2013 bude hodnota stejného spotřebního koše vyšší o 320 Kč. Tento nárůst byl velmi ovlivněn zvýšením DPH od ledna 2013.

Cena vstupů. Pokud dodavatel prodává materiál za vyšší ceny na vstupu, negativně to ovlivní ceny upraveného materiálu či zboží na výstupu. Ceny se zvýší a přenáší riziko na obchod podniku. Cena vstupů se týká i informačního systému a ostatních aplikací, například z hlediska licence na jednoho zaměstnance. Náklady se mohou nepříznivě promítnout do ceny na výstupu.

Ceny energií. Z pohledu mateřského podniku sídlící v USA, je cena energií nesmírně důležitý faktor, který ovlivňuje ceny na výstupu. Pokud jsou ceny energií vysoké, musí se promítnout do cen při dalším prodeji materiálu nebo zboží určené odběratelům. Hlavním předmětem podnikání mateřského podniku je výroba, ale předmětem činnosti posuzovaného podniku (umístěného v ČR), jsou služby ve finanční oblasti. Tato pobočka je na výrobním podniku závislá.

Cena energií v posuzovaném podniku se týká hlavně provozní činnosti v Brně, tzn. fixní náklady vynakládané na energie za provoz počítačů, osvětlení, klimatizaci apod. Tento podnik je neplatí přímo, jsou promítnuty v ceně za pronájem, která se zvýšením cen energií bude logicky také navýšena.

4.3.1.3 Společenské (sociální) faktory

Vzdělanost zaměstnanců. Požadavky na zaměstnance v tomto podniku jsou na vyšší úrovni. Požaduje se minimálně bakalářské vzdělání a rok praxe na obdobné pozici. Pokud chybí uvedené vzdělání, požaduje se dlouholetá praxe na obdobné pozici. Nejde jen o požadavek, ale lidé, kteří jsou vzdělanější, mohou mít větší přínos pro podnik z hlediska možných návrhu na zlepšení, mapování procesů apod. Lidský kapitál na vysoké úrovni, například jako jsou třeba i vědci, je mimořádně důležitý pro jakýkoliv podnik.

Demografický vývoj populace. Počet obyvatel v ČR byl v roce 2012 dle statistiky kolem 10,2 milionů. Tento trend by se měl držet zhruba stejné úrovně až do roku 2030 (27). Finanční podnik sídlí přímo v Brně, ve druhém největším městě České republiky.

Přístup k práci a volnému času. Ve všech zemích na celém světě je přístup k oběma faktorům rozdílný, podobně jako např. v České republice a Řecku. Velmi podstatné pro investora je, aby podnik, ve které zaměstnanci pracují, měl vysokou produktivitu práce, jinak jsou, investované prostředky neefektivně vynaloženy. Z průzkumu vyplynul i pozitivní přístup k práci v České republice.

Věk zaměstnanců. V České republice ve všech podnicích převládá nižší věk zaměstnanců stavu v Anglii nebo Německu. Mladí lidé jsou dnes velmi průbojní a ambiciózní vydělat s cílem maximálního výdělku. Problémem je na druhé straně jejich nezkušenost a někdy i neprofesionální přístup, což je rozdíl oproti zaměstnancům staršího věku.

4.3.1.4 Technické (technicko-technologické) faktory

Celkový stav technologie. V případě podniku a poskytovaných finančních služeb výrobním pobočkám v zemích EU je nezbytné, abychom vlastnili bezproblémový hardware v případě počítačů a serveru, a také efektivní software, což je v tomto případě vhodný informační systém a ostatní podpůrné aplikace pro práci. Hardware nesmí brzo zastarávat a software by měl mít nejlépe dokonalou podporu a být neustále aktualizován.

Rychlost zastarávání. Z hlediska hardware tu existuje hrozba ve smyslu opotřebení, záleží tedy na kvalitě. Software je třeba posuzovat z hlediska update a podpory. SAP je sice relativně starý informační systém, avšak má kvalitní podporu a neustálé aktualizace, takže by zde neměl být problém.

Nové objevy. Procesy pro zpracování finančních záležitostí podniku má v režii informační systém SAP spolu s dalšími podpůrnými programy. Zde mohou hrát významnou roli nové objevy jak nějaký proces urychlit, zlepšit, zjednodušit. A to není pouze v odhalení nějakého vhodného programu či jeho vytvoření na míru , ale především odstranění přebytečných kroků v procesu.

Moderní vybavení. Týká se veškerých podpůrných prostředků k vykonávání práce v podniku, ať se to týká všech kancelářských pomůcek, tak třeba i židlí určených k sezení u počítače, kde hraje důležitou roli pohodlí zaměstnance, čímž lze zabránit případným budoucím zdravotním potížím.

4.3.2 Rozbor 7S faktorů.

V této kapitole budou rozebrány faktory, jako jsou struktura, strategie, systémy, sdílené hodnoty, schopnosti, spolupracovníci a styl.

4.3.2.1 Strategie podniku

Vizí podniku je splnění všech požadavků vedoucích k uspokojení všech finančních závazků v co nejpozdějších termínech, ale maximálně ke dni splatnosti a domáhání se finančních pohledávek v co nejkratším termínu, nejlépe bez účasti faktoringové společnosti.

Strategií podniku je aktuálně co nejefektivněji zpracovávat přijaté faktury, platit dle systému uvedeného v předchozím odstavci a vydávat faktury za prodané zboží či služby se snahou rychlé úhrady peněz za dodané zboží či služby. Tato strategie je doplňována strategií diferenciace z pohledu náboru a vedení zaměstnanců v podniku. Posuzovaný podnik nekonkuruje dalšímu podniku v oboru finančních služeb, spíše si konkurují jako výrobní podnik, protože finanční oblast není v podniku outsourcována. Ale drží si vysoký standard v úrovni zaměstnanců dle úrovně vzdělání a jeho zaměření, potřebné praxe a věku, kde lze navázat i částečně se strategií minimálních nákladů z pohledu zaměstnání co nejmenšího počtu zaměstnanců. Tedy zaměření na kvalitu, až pak na kvantitu. Z toho vyplývá, že podnik si sice svých zaměstnanců váží, pokud se jedná o finanční stránku. Díky tomu pracují v podniku kvalitní zaměstnanci s vysokou efektivitou práce, což na druhé straně přináší podniku úsporu na počtu dalších potencionálních zaměstnanců a event. nákladech na ně. Tato kombinace strategií se může zdát být velmi efektivní pro top management mateřského podniku, pokud tuto situace budeme obhajovat konkrétními čísly. Celková strategie pak může spočívat ve velmi kvalitním zkušeném personálu.

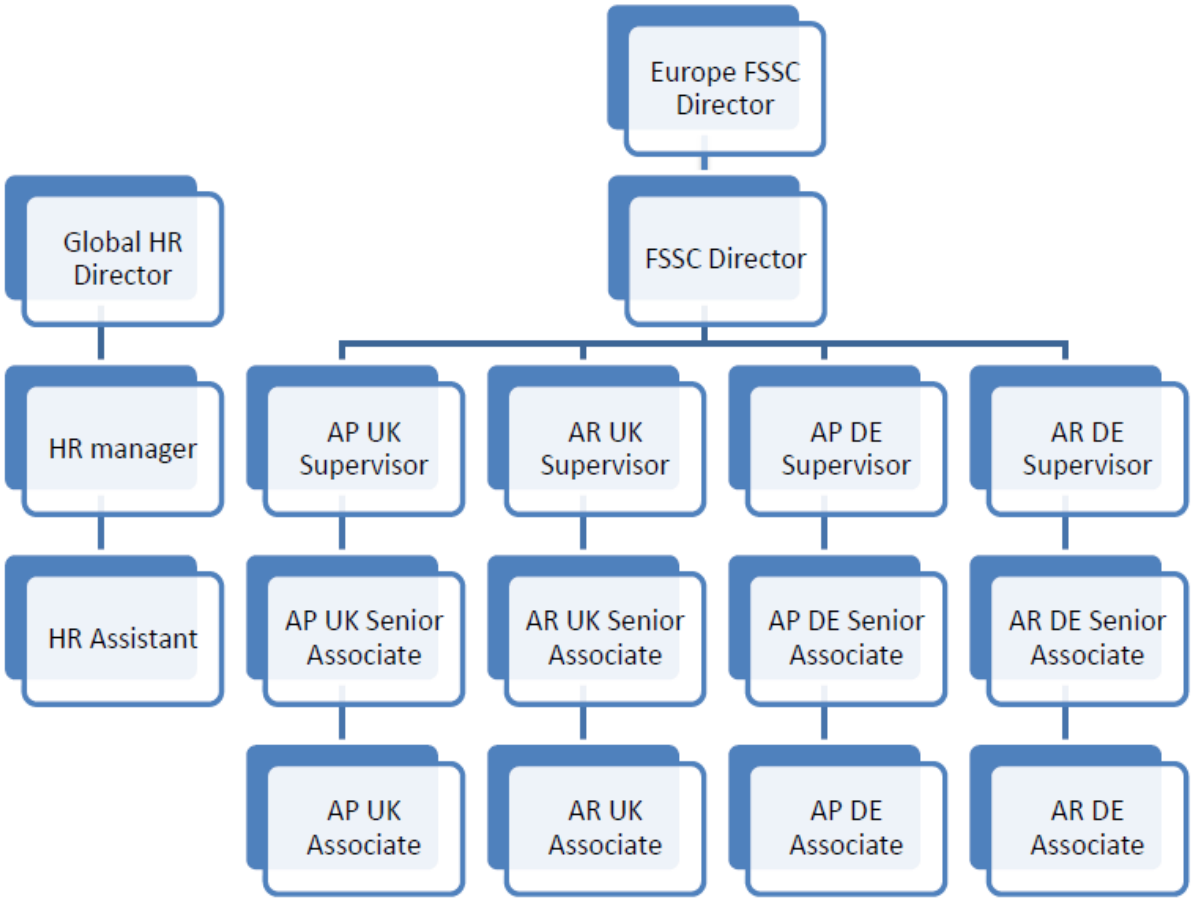
„Corporate“ strategie spočívá v podnikání ve finančním sektoru. Obchodní strategie pak soustředí své působení v přijímání a vydávání faktur, s tím spojených ostatních procesů. Z toho odvozené další strategie se týkají hlavně strategie finanční.

Předchozí strategie ale nezahrnuje problematiku bezpečnostní politiky. Jelikož podnik tuto problematiku neřeší, není to ani předmětem této strategie. V další části této práce se tato strategie bude vytvářet. Budou se muset shrnout veškeré nedostatky ohledně této problematiky, ohodnotit aktiva, určit veškeré rizika, provést opatření atd., a to vše za účasti minimálních nákladů a maximální kvality.

4.3.2.2 Organizační struktura podniku

Podnik v Brně je dceřinou společností mateřského podniku, jemuž jez hlediska řízení podřízená. Ředitel finančního podniku je podřízen řediteli mateřskému podniku působí-

cího na evropské úrovni. Řediteli tohoto podniku se zodpovídají vedoucí jednotlivých štábů, konkrétně vedoucí pro Accounts Payable (AP) oddělení a vedoucí pro Accounts Receivable (AR) oddělení pro anglický a německý tým, celkem 4 vedoucí. Pod těmito vedoucími se zodpovídají senioři a pak ostatní zaměstnanci. Personální manažer je podřízen globálnímu manažerovi mateřského podniku, to znamená, že tato osoba se nezodpovídá řediteli tohoto podniku v České republice, tak jak je uvedeno v organizační struktuře podniku na obrázku 4.3.



Obrázek 4.3: Organizační struktura podniku v České republice

Jak jsi lze všimnout, chybí zde zodpovědná osoba pro řízení a rozvoj informačních systémů, která bývá označována zkratkou CIO.

Tito zaměstnanci, senioři a ostatní zaměstnanci mají určitou specializaci a odbornost v procesech, totéž platí pro jejich vedoucí, kteří musí dokonale všechny procesy znát. Zaměstnanci na jednotlivých nejnižších úrovních poskytují rady směrem nahoru, tedy k vedoucím, a ti až dále k řediteli, což ulehčuje určitá rozhodnutí, jedná se částečně o liniově štábní strukturu.

4.3.2.3 Informační systémy

Informační systém v posuzované společnosti představuje hlavní roli ve všech podnikových procesech, které se v podniku odehrávají. Součástí jsou podpůrné systémy, které jsou s hlavním informačním systémem propojeny a ulehčují tak určité části procesů.

Hlavní informační systém SAP spolu s dalšími moduly a podpůrnými informačními systémy, které jsou s IS SAP propojeny, umožňují ulehčit některé části hlavních procesů. Jedním z nich je již zmiňovanýmodul Brainware, skládající se z dalších softwarových aplikací Onbase a Distiller Verifier.

V informačním systému SAP lze provádět mnoho funkcí, od personálních záležitostí, přes ovládání skladů až po finanční a analytické. Bez informačního systému SAP by zaměstnanci nemohli realizovat svoji činnost, a to ze dvou důvodů. Jedním z nich je propojenost mateřského a dceřiných podniků s tímto informačním systémem. Dalším důvodem je, že tento podnik zpracovává veškeré faktury a platby v tomto systému a slouží k dalším analýzám a budoucím auditům, které je nutné ze zákona provádět.

Většina procesů v SAP je automatizována, ať je to proces zpracování některých faktur pomocí podpůrných systémů nebo nahrávání obrázků, nebo dokonce i automatické platby, i když ne ve všech případech tato automatizace je reálná. Informační systém SAP má jeden veliký problém, a to je jeho špatná uživatelská přívětivost. Mnoho operací, které se musí provést, jsou zbytečně složité a některé kroky naprosto zbytečné. Uživatel musí mít mnoho znalostí, jak se dobrat k určitým operacím. Např. ke zrušení ještě nezaplacené faktury musí uživatel provést celkem tři další operace. Bohužel tento krok nelze nějak nahradit nebo zkrátit.

Co se týče procesu formování vnitropodnikových pravidel posuzovaného podniku, SAP procesů apod., tvoří se v podpůrných aplikacích, jako je Microsoft Office. Doposud se tento stav neřešil jinak. V případě globálního či mezinárodního měřítka se používá emailový klient Lotus Notes od firmy IBM, kde lze pomocí intranetu sdílet tyto dokumenty.

Doposud nejsou vytvořena žádná pravidla pro bezpečnostní politiku, tzn. jak by měl každý uživatel pracovat s daty, počítači, co lze a nelze. Přesto IS SAP může být ohrožen např. výpadkem hardware, napadením virem atd.

4.3.2.4 Styl řízení

Tento faktor není zcela jednoznačný, přesto lze říci, že se jedná o demokratický styl řízení. Vedení směřované od nejvyšších pozic v podniku je spíše autoritativní povahy stylu vedení. Avšak v týmu je tato situace poněkud odlišnější, převládá spíše styl demokratický. Vedení v týmu převládá vyšší participace zaměstnanců na řízení procesů a záležitostí s tím spojených. Komunikace je dvousměrná.

Záležitosti se probírají na poradách, kde nadřízený popíše záměr a nechá své podřízené vyjádřit k danému problému. Akceptuje reálné návrhy, dělá si poznámky, na základě kterých se případně i pak rozhoduje. Odpovědnost zůstává plně na nadřízeném pracovníkovi. Výhodou tohoto způsobu může být větší kreativita v řešení problémů a hlavně dobrý pocit sounáležitosti podřízených zaměstnanců k řešení problémů, současně tím dochází

k upevnění postoje nelhostejnosti k podřízeným pracovníkům. Tento styl řízení se může hodit i u stanovování bezpečnostní politiky, každý může navrhnout i nová opatření. Lépe se budou pravidla i zavádět, pokud panuje demokratický přístup v podniku, než autoritativní, kdy se zaměstnanců nikdo neptá a rovnou implementuje pravidla. Pak mohou ze strany zaměstnanců vznikat neetická jednání vůči zaměstnavateli v porušování pravidel nebo poškozování podniku v případě odchodu ke konkurenci.

4.3.2.5 Spolupracovníci

Spolupracovníci jsou hybnou sílou celého podniku. Jelikož se jedná o komplexní finanční služby, musí být schopni spolu vycházet. To se týká nejen zaměstnanců na vedoucí pozici, ale i podřízených zaměstnanců a mezi podřízenými a nadřízenými, nejlépe na globální úrovni, to znamená nejen v tomto podniku, ale i mezi různými pobočkami v jiných zemích. Vytváření nepřátelské atmosféry brzdí zaměstnance v pozitivním rozvoji.

Informační systém SAP je velmi komplexní, co se procesů týče, existuje zde velmi mnoho možností, jak některé procesy v praxi provozovat, některé jsou efektivnější než jiné. Právě díky zaměstnancům vznikají nové, lepší procesy, nápady, inovace a je na vedoucím pracovníkovi, aby je dostatečně motivoval. Dalším důležitým faktorem je motivace, nemůže spočívat jen ve finančním ohodnocení. V posuzovaném podniku funguje motivace v podobě jednoho týdne dovolené navíc, flexi pasy, příspěvek na školení jakéhokoliv druhu ve výši maximálně do 5 tisíc Kč. Organizují se i „teambuildingy“. Avšak neuvědomělost rizik spojených z ledabylým přístupem k bezpečnostním pravidlům může vést k ohrožení fungování IS.

Vnitropodniková, i když kvalitní školení ohledně informačních systémů probíhají pouze nárazově. Pravidelně se neprezentuje budoucí strategie, ani současná ohledně informačních systémů, což opět není ideální stav. Motivace jinou formou je velmi těžká, ke zlepšení může vést např. otevřená komunikace k tomuto tématu.

4.3.2.6 Podniková kultura

Tento podnik je multikulturní, to znamená, že v podniku nejsou pouze zaměstnanci z České republiky, ale i z jiných, a to i neevropských zemí. Momentálně zde pracují např. lidé z Rumunska, Slovenska, Polska.

Podnik je otevřený všem národnostem, pokud budou splňovat podniková očekávání. Multikultura je tu přítomna především díky realizaci finančních služeb pro různé země. Pokud je možnost zaměstnat osobu, která ovládá mateřský jazyk země, pro kterou se finanční služby provádějí, je to pro podnik určitá výhoda z pohledu komunikace a možných jazykových bariér. S multikulturním prostředím se musí každý zaměstnanec smířit a tolerovat určité případné nezvyklé situace, na které z hlediska odlišných kultur není zvyklý, přestože podniková kultura mateřské země, kde podnik působí, převažuje.

4.3.2.7 Schopnosti

Podnik se zabývá účetnictvím a obecně finančními službami, proto každý zaměstnanec musí mít adekvátní schopnosti, aby mohl svědomitě a bezchybně vykonávat svěřenou pozici v podniku. Nábor zaměstnanců je řízen dle těchto požadavků. Týká se to zaměstnanců nejen na nejnižších stupních, ale i na vedoucích pozicích.

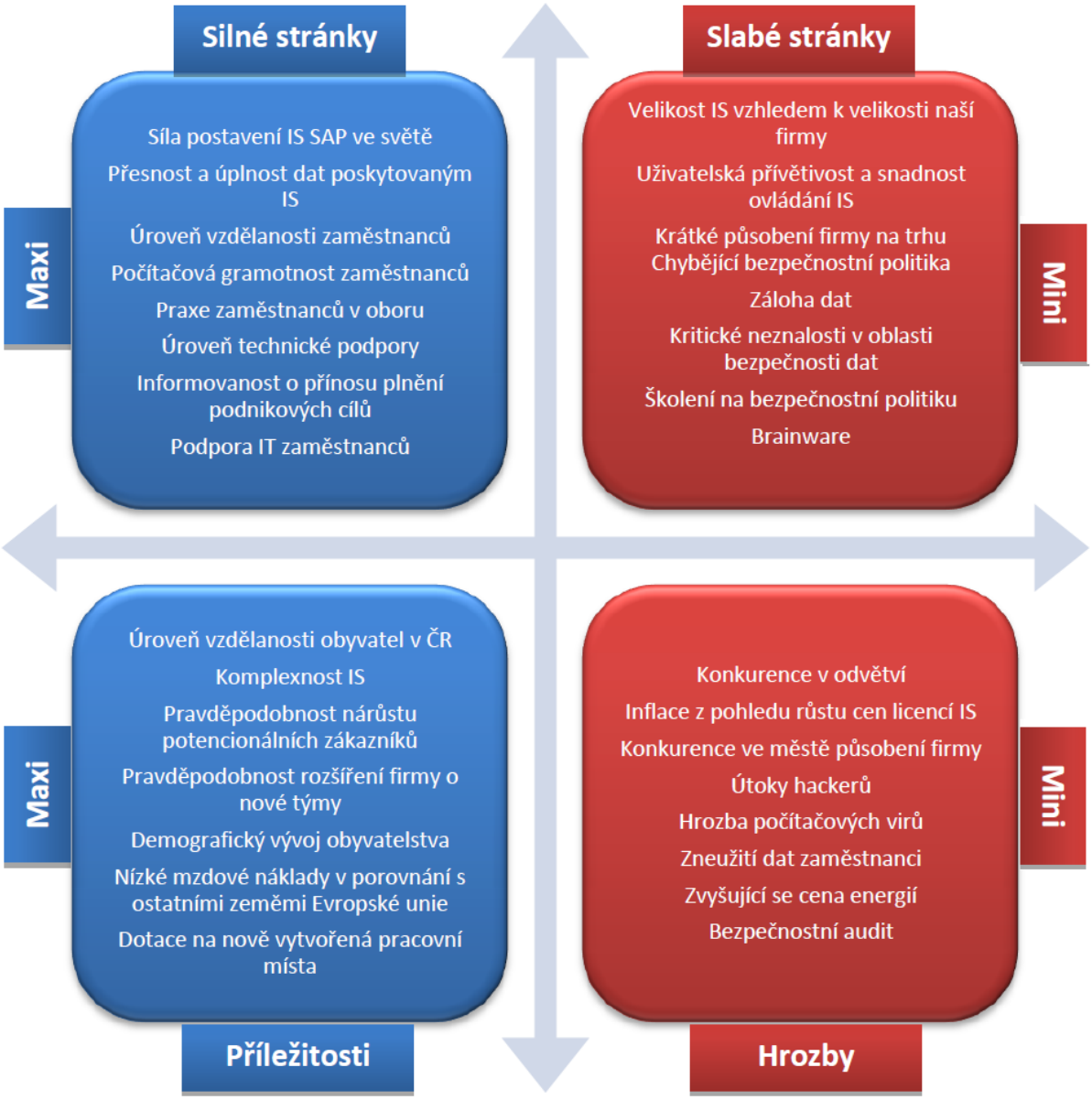
Významnou roli zde sehrávají manažerské dovednosti motivovat zaměstnance k plnění cílů jako celkového týmu a dodržování podnikových strategií ve stanovených termínech. S tím související možná vylepšení a inovace v procesech, týkající se i procesech bezpečnostní politiky. Finanční obor patří mezi obory, které se řadí k procesům, které nejsou zcela stereotypní a musí se řídit určitými finančními a bezpečnostními zákony a pravidly. V posuzovaném podniku se proces řídí podle mezinárodních standardů US GAAP, bezpečnostní politika IS chybí. Ve schopnostech vedoucích pracovníků by mělo být umění přesvědčit podřízené pracovníky k dodržování stanovených pravidel bezpečnostní politiky vedoucí k bezpečnému zajištění fungování IS za minimální pravděpodobnosti vzniku bezpečnostního incidentu.

Většina zaměstnanců již má určité zkušenosti s informačním systémem, i když ne přímo se SAP, což může být výhodou, protože mohou porovnat úroveň informačního systému z hlediska daných procesů se zvyklostmi a poznatky z předchozího informačního systému. Tyto možnosti by měl využít řídící pracovník a členy svého týmu motivovat k jejich zlepšení, být schopný adaptovat nejen sebe, ale i svoje podřízené ke všem možným změnám, které mohou v průběhu času nastat i v případě odhalení nějakých procesních nedostatků a zamezit tak možným budoucím finančním postihům.

Není možné celou dobu pracovat v určitém směru stereotypu, ale naopak vymýšlet a zkoušet nové věci, které by mohly nějakou danou situaci týkající se informačního systému vylepšit, zefektivnit, jít proti proudu, spoléhat na vlastní podvědomí a intuici. V podniku jsou i nadřízení pracovníci, kteří svým způsobem žijí pro podnik a věnují práci pro něj veškerý svůj volný čas, což je jistě pro podnik přínosem.

4.3.3 SWOT analýza

V následující analýze bude provedena analýza příležitostí a hrozeb, silných a slabých stránek. Cílem je eliminace hrozeb a slabých stránek, naopak maximální využití příležitostí a silných stránek. Na základě této analýzy budou vytvořeny určité strategie, které by mohly firmě pomoci.



Obrázek 4.4: SWOT analýza

4.3.3.1 SO Maxi - Maxi

- Propagovat výhodu nízkých mzdových nákladů oproti jiným zemím Evropské unie. Tímto způsobem by bylo vhodné rozšířit nová pracovní místa a lépe využít velikost informačního systému ve prospěch podniku a hlavně získat dotace na nově vytvořené pracovní pozice.

- Využít příležitosti rozšíření týmů o nové země (týmy) zdůvodněním vysoké úrovně vzdělanosti, tím i kvality zaměstnanců, obecně vzdělanost obyvatel České republiky.

- Z hlediska vyšší úrovně vzdělanosti potencionálních zaměstnanců a zaměstnanců v podniku lze lépe vést různá školení ohledně provozu IS SAP a bezpečnostní politiky.

- Proporcionální růst obyvatelstva v ČR a počtu vystudovaných lidí v IT oboru roste počet firem na trhu v této oblasti, z toho pohledu je vhodné lépe zmapovat IT podniky v Brně a vybrat optimální podnik z pohledu kvalita/cena.

4.3.3.2 ST Maxi – Mini

- Silné postavení IS ve světě jeho velikostí nám dává konkurenční výhodu oproti ostatním firmám, které na trhu působí, a to jednak jeho komplexností a již nabytými znalostmi zaměstnanců.

- Počítačová gramotnost zaměstnanců by mohla podpořit zamezení počítačovým útokům z venčí, to musí být podpořeno i vhodným výběrem antivirového programu a firewallu, dále i podporou IT zaměstnanců externího podniku.

- Informovanost o přínosu plnění podnikových cílů z pohledu bezpečnostní politiky by měla zamezit zneužití podnikových dat zaměstnanci, tedy eliminace útoku zevnitř.

- Podporu IT zaměstnanců lze využít v případě bezpečnostního auditu, zvláště pokud v podniku pracují od vzniku společnosti, dokud se nebude analyzovat situace ohledně vhodnosti náboru CIO.

4.3.3.3 WO Mini – Maxi

- Využití velikosti IS nárůstem potencionálních zákazníků, rozšíření dosavadních týmů, vznik nových pracovních míst, získání dotací k tomu účelu.

- Neduh uživatelské přívětivosti a složitosti ovládání IS lze eliminovat nalezením vhodného modulu či nástavby IS SAP a vypořádat se i tak s nevyhovujícím systémem Brainware.

- Jelikož úroveň vzdělanosti v České republice je na dobré úrovni, je velmi důležité, aby se tato vzdělanost bez pochyby rozšířila o vznik detailní bezpečnostní politiky a eliminovala se tak kritická neznalost v oblasti bezpečnosti dat.

- S předchozím bodem souvisí pravidelná školení o bezpečnostní politice formou ústní prezentace, dále aby podnikem pověřená osoba propagovala různé formy prezentace bezpečnostní politiky, jako jsou informační emaily, nástěnky, využití novinek na intranetu apod.

4.3.3.4 WT Mini – Mini

- Je nutné zavést bezpečnostní politiku, aby se eliminovala kritická neznalost v oblasti bezpečnosti dat zaměstnanců podniku a předešlo se tak i útokům z vnějšího prostředí v podobě zásahu hackerů, počítačových virů, zneužití dat apod.
- Lepší motivace zaměstnanců z pohledu krátkého působení podniku na trhu. Existuje konkurence, která je tu delší dobu a může získávat kvalitní zaměstnance z posuzovaného podniku, což může být z pohledu risk managementu kritické.
- Hrozba rostoucí inflace a DPH může negativně ovlivnit cenu licencí všech aplikací včetně IS, dále růst cen energií a s tím spojený nárust cen pronájmu prostor.
- V případě rizika prozrazení vnitropodnikových informací při odchodu/přeplacení zaměstnance ke konkurenci by bylo vhodné ošetřit smlouvu tak, že by zaměstnanec musel respektovat pravidlo mlčení pojištěné vysokou sankcí v případě porušení.

4.4 Lewinův model

Ke způsobu řízení změn bude využit jedna z nejstarších metod, Lewinův model, který v sobě zahrnuje určitou sociální skupinu. Ze všech dosavadních analýz vyplynulo, že IS má více nedostatků, které by měly být napraveny, například bezpečnostní politika, špatná uživatelská přívětivost a poměrně obtížná ovladatelnost IS SAP, či modul na zpracování faktur Brainware propojený s IS SAP. Nejvíce rizikový faktor z pohledu celého IS je nutnost zaměřit se čistě jen na chybějící bezpečnostní politiku. V případě problematiky bezpečnostní politiky je možné se ještě zamyslet nad zvolenou metodou řízení změny, a to buď reengineering, který se zaměřuje na celkový redesign podnikových procesů, a i když tato metoda se spíše zaměřuje na čistě technické procesy IS SAP, z pohledu tohoto podniku by to byly procesy týkající se finanční stránky procesování faktur, plateb atd. Proto byla zvolena metoda Lewinova modelu, který v sobě zahrnuje sociální skupinu ohledně změny.

4.4.1 Síly inicializující proces změny

Jak bylo uvedeno, změna informačního systému jako takového není možná, změna aplikace Brainware není prioritou, problém se zpracováním všech druhů faktur byl vyřešena způsobem minimálního zatížení této aplikace. Proto budeme posuzovat jen bezpečnostní politiku z pohledu tohoto podniku, kdy výsledkem analýzy je rozhodnutí:

- **Bezpečnostní politika** - současný stav je *nevyhovující!*

Na základě výše uvedeného rizikového faktoru je nutné v bezpečnostní politice provést změnu zásadního charakteru s cílem eliminovat negativní dopady její neexistence v podniku.

4.4.1.1 Síly působící pro plánovanou změnu

- Zainteresované kvalitní vedení, které se bude v dané věci maximálně angažovat.
- Softwarové vybavení včetně aktualizací.
- Finanční prostředky.
- Vnitropodniková školení.
- Vzhledem k průměrnému nízkému věku v podniku, ochota učit se novým věcem.
- Kvalitní podpora externích IT pracovníků.
- Kvalitní zaměstnanci.

4.4.1.2 Síly působící proti plánované změně

- Neochota zaměstnanců dodržovat stanovená pravidla.
- Neochota zaměstnanců přejít na nový systém bezpečnostní politiky.
- Možné obtíže s přesvědčením klíčových manažerům k plánovaným změnám, zvláště v případě nových investic.
- Neochota zaměstnanců účastnit se plánovaných školení.
- Neprofesionální přístup.
- Volba nevhodné bezpečnostní politiky.
- Časová bariéra implementace nových změn.

4.4.2 Identifikace agenta změny

Sponzorem změny bezpečnostní politiky informačního systému SAP bude ředitel podniku, pokud se jedná o finanční stránku nutných interních změn bezpečnostní politiky. Agentem změny bezpečnostní politiky bude skupina vedoucích pracovníků, tedy management. V tomto podniku pracují čtyři vedoucí pracovníci s určitými analytickými schopnostmi, které jsou na této pozici nezbytné a každý z těchto vedoucích pracovníků má nejlepší přehled o svém týmu podřízených pracovníků a může tak nejlépe identifikovat stupeň očekávaného osobního rizika a stupeň nespokojenosti se současným stavem.

Benevolence zaměstnavatele umožňuje zaměstnancům mnoho aktivit, kde ne všechny by měly být povoleny, např. zcela volný přístup k internetu, připojení flash disku, instalace libovolných programů atd. Většina zaměstnanců nebude chtít pravděpodobně stanovená pravidla vnitřně dodržovat. V tomto případě očekáváme proto nízkou akceptaci očekávaných změn, tedy nízkou nespokojenost se současným stavem a vysoké očekávané osobní riziko plynoucí ze změny. Pracovníci tedy budou muset být nějakým způsobem motivováni, aby se dostali do sektoru vysoké akceptace očekávané změny.

4.4.3 Identifikace intervenčních oblastí

Zásahy, které se budou týkat změn bezpečnostní politiky, se budou týkat těchto oblastí:

- Komunikační a organizační toky.

V případě vytvoření optimální bezpečnostní politiky se změní osobní svoboda zaměstnanců, nejvíce bude ovlivněna skupina podřízených zaměstnanců. Bude se muset omezit přístup na internet, zakázat přístup nekontrolovatelného připojování flash disků a jiných datových nosičů, zprovoznění zálohy dat počítačů zaměstnanců, povolení instalování programů pouze v administrátorském prostředí, vytvoření návodu, jak individuální data v počítači chránit.

Tato změna by byla provedena za asistence externího IT podniku spolu s týmem vedoucích pracovníků, kteří by pak předávali získané poznatky svým podřízeným. Na vedoucích pracovnících by pak bylo, jak své podřízené motivují k dodržování bezpečnostní politiky a jak eliminují kritickou neznalost v oblasti bezpečnosti dat.

Informace by pak byly distribuovány všemi komunikačními kanály, vhodné by bylo vypracovat dodatek ke smlouvě o bezpečností politice s podpisy všech zaměstnanců v podniku.

4.4.4 Intervence – vlastní změna

Vlastní změna by měla probíhat podle předem naplánovaných činností, které musí být vzájemně provázané.

4.4.4.1 Fáze rozmrazení

Ve fázi rozmrazení je nutné identifikovat současnou úroveň zavedených pravidel a připravit je na změnu. V současné době neexistuje žádné psané pravidlo pro chování zaměstnance ve věci bezpečnostní politiky informačního systému. Nikdy se o této problematice příliš nehovořilo, spíše trvá stav, kdy závisí na každém zaměstnanci, jaké rizikové postavení zaujme, pracuje-li s IS počítačem a jeho okolím, protože neexistuje osoba, která by dohlížela na dodržování všeobecných bezpečnostních pravidel uvedených v pracovní smlouvě. Bezpečnostní pravidla jsou v podniku tedy na minimální úrovni, ohrožení je zde vysoké. Proto je potěšující a žádoucí příprava zavedení nového procesu bezpečnostní politiky.

4.4.4.2 Vlastní změna

Vytvoří se nová bezpečnostní politika. Před implementací a zapojením agentů změny při školení cílové skupiny se proces odstartuje ohodnocením jednotlivých aktiv podniku z hlediska potencionálních rizik, po ohodnocení se vytvoří předběžná opatření a stanoví se procesy uplatňování bezpečnostní politiky v praxi tak, aby jim zaměstnanci co nejlépe rozuměli. Byl by to soupis, který vymezí, chování k IS, aby nedošlo k bezpečnostnímu incidentu. Mělo by to zahrnovat nejen samotný IS SAP, ale i jeho okolí. Ohodnocení jednotlivých bezpečnostních prvků bude provedeno též mimo zaměstnaneckou úroveň, například posouzením vhodnosti antivirové ochrany, bezpečnosti přístupu do prostor pracoviště apod. Případné nedostatky budou napraveny, zde může být řešena i finanční stránka. Po stanovení všech těchto činností, pomocí stochastického modelu, bude vytvořena bezpečnostní politika jako celek, prezentovaná agentem změny, který bude zodpovědný za její implementaci.

Po vypracování nové bezpečnostní politiky dojde k šíření pomocí komunikačních kanálů, jako je intranet, nástěnka a jedno nárazové velké školení, kde každý zaměstnanec dokument podepíše jako dodatek ke smlouvě. Pak lze formou emailů, nástěnek, školení a testů udržovat v podvědomí každého zaměstnance informace ohledně bezpečnostní politiky.

4.4.4.3 Fáze zamrazení

Po implementaci pravidel bezpečnostní politiky IS je nutné zjistit dosažené výsledky a porovnat je s předchozím stavem. Musí být zjištěna spokojenost zaměstnanců, vedení se zavedenými změnami a výsledky změn. Jelikož tahle situace se bude asi obtížně porovnávat, a to i proto, že před stavem implementace téměř neexistující bezpečnostní politiky se žádné vyhodnocení neprovádělo. Proto se jako předchozí stav dá ohodnotit nulovými hodnotami a pro další ohodnocení lze použít KPI. Lze zavést metrickou tabulku, kde se budou náhodně vybírat zaměstnanci a bude se posuzovat dodržování stanovených pravidel bezpečnostní politiky IS. Ideální by byla nezávislá osoba, např. CIO, který by měl bezpečnostní politiku na starosti.V případě výběru jiného zaměstnance z daného týmu takový typ kontroly může vytvářet nepřátelské prostředí.

V případě spokojenosti s dosaženými výsledky pak musí dojít k tzv. zamrazení změny a fixaci dosažených výsledků. V takovém případě lze konstatovat, že implementace byla úspěšná a nezbývá než udržovat minimálně stejnou úroveň, optimálně proceduru postupem času aktualizovat a neustále zlepšovat, k čemuž lze právě Lewinův model opakovaně používat.

4.5 Bezpečnostní politika

Nejdříve je nutné provést identifikaci a ohodnocení aktiv, které informační systém ovlivňují přímo i nepřímo. Proč je vhodné všechna tato aktiva analyzovat? Pokud by tato práce byla zaměřena pouze na analýzu aktiv, hrozeb, rizik, které ovlivňují jen informační systém a nebyl by brán ohled na všechny faktory, tedy i ty které ovlivňují IS ze vnějšku, potenciální rizika by byla neúměrně vysoká.

4.5.1 Identifikace aktiv

Nejprve bude provedena identifikace aktiv, tzn. rozdělení veškerých aktiv, která s informačním systémem nějakým způsobem souvisí. Aktiva jsou rozdělena do třech hlavních skupin, a to finančního, hmotného a nehmotného majetku. Tyto skupiny budou nadále děleny na podskupiny a následně ohodnoceny.

Identifikaci **hmotného majetku** si lze rozčlenit mezi najímané prostory, počítače, notebooky, monitory a další počítačové vybavení, kancelářské potřeby, kancelářský nábytek, místnost se servery, tzv. „serverovna“, dále pak zařízení ovlivňující klimatické podmínky na pracovišti, telefony, mobily, tiskárny, řezačku dopisů, obálkovací stroj, osvětlení, vybavení kuchyně, označení jednotlivých týmů, požární systém, nástěnky, tištěné faktury, archivní materiál, výplatní pásky, ostatní dokumentace, pokladna.

Mezi **nehmotný majetek** lze zařadit software, know-how, goodwill, image podniku, faktury v elektronické podobě. Předmětem **finančního majetku** jsou pak stravenky, flexipasy, dodávané energie a voda. Z předchozího odstavce je patrné, že bude nejvíce zastoupena skupina hmotného majetku, avšak hodnota těchto aktiv v porovnání s jinými skupinami může být rozdílná. Následně bude provedeno zestručnění těchto skupin a proveden krátký popis nezbytný pro další krok této analýzy.

4.5.1.1 Hmotný majetek

- **Počítače** - důležitý prvek výbavy podniku, sloužící jako prostředek při práci s informačním systémem. Jedná se o velmi důležité aktivum, bez kterého není možno s IS pracovat, proto se mu musí věnovat více pozornosti. Hodnotí se spolehlivost a rychlost.

- **Notebooky** - podobný prvek jako počítače, notebooky mají vedoucí pracovníci, které používají nejen k výkonu své práci v daném podniku, ale i ke služebním cestám, z tohoto hlediska se vystavují dalším rizikům a hrozbám.

- **Periferie** - sem řadíme monitory, počítačové myši, klávesnice, tiskárny, pevné telefony, headsety, obálkovací zařízení, řezačky na dopisy.

- **Serverovna** - místnost, která je vybavená hardwarem pro přenos a zálohu dat v případě nějakého incidentu. Tato místnost, která je v neustálém provozu, by měla být

neustále nějakým způsobem udržována, klimatizována. Vstup do ní by měl být vymezen autorizací přístupů osob, kvalitním připojením a dodávkou energií atd.

- **Infrastruktura** - budova, vhodnost najímaných prostor pro firemní účely, dále přístup do těchto najímaných prostor, tzn. ostraha objektu, autorizovaný přístup do prostor podniku.
- **Kancelářské potřeby** - tužky, lepící pásky, sešívačky, nůžky, pravítka, pořadače na dokumenty, šanony a další. Tato podskupina je skupinou podpůrnou k vykonávání hlavní činnosti s informačním systémem SAP.
- **Mobilní telefony** - tato podskupina není záměrně zařazena v podskupině periferie. Důvod je ten, že podnikové mobily vlastní jen vedoucí pracovníci a nejsou tedy na jednom pevném místě. Vedoucí pracovníci je mohou využívat mimoslužebně, na služebních cestách. Jsou v nich uloženy citlivé údaje, jako např. podnikové emaily.
- **Podnikové prostředí** - týká se vhodného a dostatečného osvětlení, zároveň ochrana před slunečním zářením, v zimě topení, v létě fungující klimatizace. Všechny tyto prvky musí fungovat, aby zaměstnanci mohli pracovat ve vhodném firemním prostředí. Patří sem i označení týmů cedulkami a malými vlajkami rozlišujícími země, což zvyšuje přehlednost.
- **Kancelářský nábytek** - vhodně řešený kancelářský nábytek, jejich prostornost a optimální rozmístění v prostorách podniku.
- **Tištěné faktury** - neboli „hardcopies“ faktury, což jsou faktury v papírové formě, které došly poštou nebo byly vytisknuty zaměstnancem podniku z elektronického zdroje. Zneužití faktur může být velmi rizikové, stejně tak i špatné zpracování. Má to negativní dopad na goodwill podniku. Archivace faktur je součástí této podskupiny.
- **Kuchyňské vybavení** - místnost, kde se stravují zaměstnanci, je vybaveno kuchyňskou linkou, mikrovlnými troubami, nádobím, příbory atd. Je logické, že tato podskupina bude IS ovlivňovat naprosto minimálně.
- **Bezpečnostní zařízení** - turnikety a s tím spojená autorizace přístupů do různých částí firemních prostor, hlásiče požáru, hasicí přístroje, kamery, bezpečnostní východy.
- **Ostatní dokumentace** - sem patří ostatní dokumentace, jako jsou procesní dokumenty, smlouvy se zaměstnanci, výplatnice, dokumenty obsahující různé směrnice atd., včetně jejich archivace.

4.5.1.2 Nehmotný majetek

- **Informační systém** - velmi důležitá podskupina, kam patří informační systém SAP, bez kterého nelze provádět pracovní činnost. Veškerá rizika spojená s IS nelze brát na lehkou váhu a je třeba všem rizikům věnovat maximální pozornost.

- **Podpůrný software** - tento software slouží k podpůrné činnosti s informačním systémem SAP. Patří sem operační systém, Brainware, který je s IS SAP přímo propojen, dále IBM Lotus Notes, Microsoft Office 2007 Professional a antivir Symantec.

- **Data** - jakákoliv data spojená s IS SAP, ať už to jsou data přímo v informačním systému nebo data uložená mimo IS. Jakákoliv podniková data jsou nesmírně citlivá a mohou být lehce zneužita. Únik dat je velmi nákladný.

- **Know-how** - veškeré znalosti podniku a jejich zaměstnanců, nejen těch abstraktních, ale i dokumentací k jednotlivým procesům, způsoby provádění procesů atd., patří k velmi důležitým aktivům podniku, zvláště pak know-how práce s IS SAP propojeného s účetními standardy US GAAP.

- **Služby** - jedná se o veškeré služby poskytované zaměstnanci podniku ze dvou pohledů, a to poskytování služeb dodavatelům, jako je příjem faktur, jejich zpracování a poté jejich zaplacení, řešení všech nesrovnalostí a poskytování všech informací spojených s objednávkami dodavatelům. Druhá strana je pak posuzována z hlediska prodeje, tedy oddělení, které vydává faktury, odesílá informace prodejnímu týmu a nakonec přijímá platby od odběratelů. S tím je spojené i poradenství a řešení problémů s odběrateli. Z toho vyplývá, že kvalifikace zaměstnanců zde bude hrát velkou roli. Částečně sem patří i služby poskytované podporou IT zaměstnanců ohledně IS a externích pracovníků IT podniku. Tyto poslední dvě služby jsou součástí tohoto aktiva.

- **Goodwill** - v podstatě se jedná o finanční vyjádření hodnoty podniku vypočítané z rozdílu hodnoty celkových aktiv a závazků. Čím vyšší závazky, tím horší situace pro podnik. Pokud z nějakého důvodu roste objem nezaplacených faktur, roste i hodnota závazků. Tento ukazatel může být i sledován případnými investory.

- **Image podniku** - tato podskupina je odlišná od podskupiny goodwill v mnoha případech. U podniku se jedná o vnímání značky podniku všemi stakeholdery a shareholdery.

- **Elektronické faktury** - neboli „softcopies“ faktury, jsou faktury v elektronické podobě. Má to mnoho výhod, podnik ušetří nemalé peníze za tonery, papíry a poštovní náklady, dodavatel může formát elektronické faktury šifrovat pro případ zneužití druhou nebo třetí stranou, rychlost dodání faktury je bezkonkurenční a hlavně je možné tak ušetřit peníze za poštu. Elektronickou fakturu lze zpracovat, aniž by ji bylo nutné tisknout. Všechny tyto výhody z pohledu dodavatele platí i pro tento podnik, která vystupuje na stejné pozici (Accounts Receiveables). Dnešním trendem v této oblasti je využití možnosti e-Billing, kdy se využije služeb externího podniku, který faktury archivuje, zákazník si je může vyzvednout na základě přiděleného loginu a hesla. Výhoda je opět v šetřených nákladech na tisk faktur, poštu. Faktury lze vyzvednout i později, ale pak už dochází ke zvýšení nákladů na využívání služeb

této externí společnosti. Proto je vhodné využití možnosti IS SAP k automatickému zasílání elektronických, digitálně podepsaných faktur přímo k odběrateli.

4.5.1.3 Finanční majetek

- **Cenné papíry** - sem lze zařadit zaměstnanecké bonusy, jak jsou stravenky a flexipasy. Obě varianty pro zaměstnance znamenají větší motivaci v podniku zůstat, k tomu tyto výhody podporují českou ekonomiku, mají tedy dvojí pozitivní účinek. Jejich přítomnost či nepřítomnost IS SAP zásadním způsobem neovlivní.

- **Energie** - dobrý poskytovatel, hlavně z hlediska spolehlivosti, je pro podnik velmi důležité, aby počítače, především servery, správně fungovaly. Jakýkoliv výpadek může extrémně narušit chod podniku a prohloubit tak finanční ztráty.

- **Stočné** - dodávka vody plní hlavně funkci bezúplatného občerstvení zaměstnanců, je nutná i pro ostatní potřeby. Ovlivnění IS je minimální.

4.5.2 Ohodnocení aktiv

Ohodnocení aktiv společnosti bude vycházet ze skupin a podskupin identifikace aktiv. Na základě subjektivního posouzení budou jednotlivá aktiva ohodnocena na stupnici od 1-5, kde číslo 5 bude znamenat nejdůležitější aktivum pro daný podnik. Posuzovat se budou jednotlivé aspekty aktiv, jako je důležitost, integrita a finanční ztráty pro podnik. Posuzovány budou z hlediska informačního systému SAP, ať už se jedná o aktivum, které je spjato s IS SAP přímo nebo nepřímo, budou se posuzovat dohromady. Na základě těchto měrných veličin bude proveden aritmetický průměr zaokrouhlený na dvě desetinná místa sloužící jako ukazatel hodnoty aktiva společnosti. Na základě tohoto ohodnocení bude vytvořena tabulka, ve které budou zvoleny intervaly ohodnocení aktiv sloužící k jednoduchému rozlišení vážnosti dopadu vyřazení aktiv z provozní činnosti.

Interval hodnot	**Úroveň dopadu**
(0,0 - 1,5>	Dopad na IS a podnik je zanedbatelný
(1,5 - 2,5>	Nízký dopad na IS a podnik
(2,5 - 3,5>	Znatelný dopad na IS a podnik
(3,5 - 4,5>	Značné potíže fungování IS a podniku
(4,5 - 5,0>	Existenční dopad na IS a podnik

Tabulka 4.1: Rozsah stupnice úrovně dopadu

Z tabulky 4.1 je patrné, že podnik by se měl soustředit hlavně na poslední dva intervaly v tabulce, kde tato aktiva mohou zásadním negativním způsobem ovlivnit fungování podniku v České republice. V následujících tabulkách bude provedeno ohodnocení hmotného, nehmotného a finančního majetku.

Číslo	HMM	Důležitost	Integrita	Finanční ztráty	$\sum$ aktiva	Hodnota aktiva
1	Počítače	5	5	4	14	4,67
2	Notebooky	4	5	3	12	4,00
3	Periferie	4	3	3	10	3,33
4	Serverovna	5	5	5	15	5,00
5	Infrastruktura	2	1	3	6	2,00
6	Kancelářské potřeby	1	1	2	4	1,33
7	Mobilní telefony	1	1	2	4	1,33
8	Podnikové prostředí	2	1	3	6	2,00
9	Kancelářský nábytek	2	1	3	6	2,00
10	Tištěné faktury	5	5	1	11	3,67
11	Kuchyňské vybavení	1	1	3	5	1,67
12	Bezpečnostní zařízení	1	1	2	4	1,33
13	Ostatní dokumentace	2	3	1	6	2,00
$\sum$	$H\bar{M}M$	2,85	2,77	2,77	-	**2,64**

Tabulka 4.2: Ohodnocení hmotného majetku

Z tabulky 4.2 se nejrizikovější skupinou staly počítače a serverovna. Další velmi rizikovou skupinou jsou notebooky a tištěné faktury. Vyčíslení finanční ztráty není posuzováno na konkrétních finančních číslech, jednak z důvodu, že podnik tyto informace neposkytuje. Dále pak i z důvodu, že nehmotný majetek lze jen těžko finančně ohodnotit, proto jsou tato čísla odhadnuta na základě konzultace odborného hodnocení s podnikem.

Z tabulky 4.3 se nejrizikovější skupinou staly IS SAP, data, know-how a služby. Další velmi rizikovou skupinou jsou podpůrný systém a elektronické faktury. Pokud porovnáme tuto tabulku s tabulkou 4.2, přestože v tabulce 4.3 je ohodnoceno podstatně méně aktiv, vyskytuje se zde mnohem více rizikových aktiv pro podnik a IS. To je způsobeno tím, že podnik je na IS postaven, s tím jsou spojena data a znalosti, jak s těmito daty co nejefektivněji pracovat a poskytovat tak kvalitní služby ve finančním sektoru podniku. I střední hodnota nehmotného majetku zde dosahuje hodnoty 4,04. To je poněkud více jak u hmotného majetku, avšak tato situace je částečně ovlivněna i menším počtem ohodnocených aktiv. Tím, že se zde vyskytuje několik rizikových skupin neznamená, že by se měl podnik soustředit pouze jen na tyto skupiny, musí věnovat pozornost všem aktivům, avšak musí svoji pozornost optimálně rozložit, k čemuž mohou tyto tabulky napomoci. Z poslední tabulky 4.4 se stala jedinou a zároveň v této kategorii nejrizikovější skupinou energie. Z těchto třech aktiv je hodnota tohoto aktiva oprávněná, protože bez přívodu energie nefungují počítače ani IS SAP. Výpadek proudu patří k těm nejhorším možným incidentům, které mohou nastat, pokud podnik nemá záložní zdroje. Celková střední hodnota zde na-

Číslo	NMM	Důležitost	Integrita	Finanční ztráty	$\sum$ aktiva	Hodnota aktiva
1	IS SAP	5	5	5	15	5,00
2	Podpůrný software	5	4	4	13	4,33
3	Data	5	5	5	15	5,00
4	Know-how	5	5	4	14	4,67
5	Služby	5	5	5	15	5,00
6	Goodwill	1	2	5	8	2,67
7	Image podniku	1	1	4	6	2,00
8	Elektronické faktury	5	5	1	11	3,67
$\sum$	$N\bar{M}M$	4,00	4,00	4,13	-	**4,04**

Tabulka 4.3: Ohodnocení nehmotného majetku

bývá hodnoty 3,01. Je to nejmenší hodnota ze všech porovnávaných skupin aktiv. Všem rizikům vycházejících z posledních dvou nejrizikovějších skupin je nutno věnovat zvýšenou pozornost.

Číslo	FIM	Důležitost	Integrita	Finanční ztráty	$\sum$ aktiva	Hodnota aktiva
1	Cenné papíry	3	1	4	8	2,67
2	Energie	5	5	5	15	5,00
3	Přípojka vody	1	1	2	4	1,34
$\sum$	$F\bar{I}M$	2,34	2,34	3	-	**3,01**

Tabulka 4.4: Ohodnocení finančního majetku

4.5.3 Analýza hrozeb

Na základě předchozí kapitoly, kde byla ohodnocena aktiva, budou identifikovány potencionální hrozby, jejich pravděpodobnost vzniku a následně z toho vyplývající zranitelnost daných aktiv, z kterých hrozby vyplývají. S těmito hodnotami se pak bude nadále pracovat, až do dosáhnutí bodu vytvoření nové bezpečnostní politiky, což bude předmětem kapitoly vlastních návrhů řešení včetně metody PERT, kde bude odhadnuta délka celého projektu.

Hrozby, které ohrožují aktiva podniku budou rozděleny do skupin hrozeb přírodních a fyzických, skupiny technické, technologické a lidské. Některé hrozby mohou být společné pro několik aktiv. Následné hrozby budou zkoumány pouze u dvou nejrizikovějších skupin.

V tabulce 4.5 jsou identifikovány hrozby, ohodnocena pravděpodobnost jejich vzniku a na základě toho je ohodnocena zranitelnost aktiv, což znamená, do jaké míry může tato hrozba dané aktivum poškodit. Hodnoty jsou stanoveny opět na základě odborného odhadu, vycházejícího z tabulek A.5 a A.6. Z tabulky je patrné, že spousta hrozeb je pro mnoho aktiv společných, selhání hardware a software, zastaralost hardware, krádež, zlomyslné kódy, výpadky sítě, požár, vnější útoky, zpronevěření aktiv a neúmyslná modifikace. Jediná hrozba, která se neopakuje, je selhání komunikace a epidemie.

V krátkém shrnutí by bylo vhodné hrozby velmi krátce vysvětlit. *Selhání hardware* nebo software je vcelku jasné, je to vyřazení z provozu nebo částečná porucha, která hlavní činnost určitým způsobem omezuje. Může to být i náchylnost zařízení na vlhkost, prach a špínu. *Zastaralost hardware*, která může vést k předchozí hrozbě, tedy k selhání hardware. Jedná se o časové opotřebení aktiva. *Požár* má vždy devastující účinky, může vzniknout zkratem nebo neodborným zacházením s hardware nebo neprofesionálním chováním. *Krádež* je dnes bohužel běžnou věcí, notebook na cestách lze odcizit mnohem snadněji než počítač v kanceláři, protože tam je omezen přístup. *Výpadky sítě* se čas od času stávají, ale měly by být minimální. Dostupnost serveru by měla být alespoň 99,9 % za rok. Z tohoto pohledu je hodnocena lokální serverovna, i když by měly být hodnoceny serverovny v USA a Německu, ale ty nejsou předmětem aktiv tohoto podniku a navíc je ani tento podnik nemůže nějak fyzicky ovlivnit, může pouze žádat o nápravu. Výpadky sítě jsou zodpovědností dodavatele a pronajímatele prostor. *Vnější útoky* je úmyslná lidská činnost s úmyslem podnik nějakým způsobem poškodit. Může to být úmyslná modifikace dat, hackerství, odposlech, DoS útoky, Zombies atd. *Neúmyslná modifikace* patří mezi neúmyslné lidské činnosti vedoucí k poškození podniku, což jsou například chyby zaměstnanců při procesování nebo nedostatečný výcvik bezpečnosti. *Zpronevěření aktiv* je zvláštní skupina trestné úmyslné lidské činnosti, kde soubor určitých činností kombinující několik hrozeb najednou vede k odcizení majetku podniku. *Zlomyslné kódy* jsou viry, červi, malware a mnoho dalších. Tento jev může být způsoben například nedostatečnou aktualizací software na ochranu před zlomyslnými kódy. *Selhání software* je nefunkčnost daného software, například crash operačního systému, což může být způsobeno mnoha příčinami. Dále to může být neodborné zacházení se software.

Selhání komunikace je závažná skupina v případě aktiva služeb. Poškození tohoto aktiva může ovlivnit goodwill a image společnosti. Velmi záleží na kvalifikaci a profesionálním chování zaměstnanců, jejich přístupu k práci. Tato komunikace se týká nejen zaměstnanců uvnitř společnosti, ale i komunikace s vnějším prostředím, jako jsou například dodavatelé a odběratelé. Poslední hrozba je epidemie, která v případě propuknutí může ovlivnit fungování IS SAP jako takového, bez lidí nemůže fungovat ani sám IS.

Ještě se zde vyskytují další hrozby, jako je zemětřesení, povodně, teroristické útoky, sopečná činnost, nepokoje, stávky. Avšak vzhledem k umístění pracoviště je pravděpodobnost výskytu velmi nízká a posuzované aktivum stěží ovlivní, proto s těmito hrozbami nemá smysl dále kalkulovat.

Číslo aktiva	Aktivum	Číslo hrozby	Hrozba	Skupina hrozeb	Pravděpodobnost vzniku hrozby	Zranitelnost aktiva
1	Počítače	1	Poruchy hardware	Technické	4	5
		2	Zastaralost hardware	Technické	3	3
		3	Požár	Přírodní	2	5
2	Notebooky	4	Poruchy hardware	Technické	4	5
		5	Zastaralost hardware	Technické	4	3
		6	Krádež	Lidské	2	4
		7	Požár	Přírodní	3	5
3	Serverovna	8	Poruchy hardware	Technické	3	5
		9	Zastaralost hardware	Technické	3	4
		10	Výpadky sítě	Technické	4	4
		11	Vnější útoky	Lidské	2	5
		12	Požár	Přírodní	2	5
4	Tištěné faktury	13	Neúmyslná modifikace	Lidské	2	3
		14	Zpronevěření aktiv	Lidské	2	3
		15	Požár	Přírodní	2	5
5	IS SAP	16	Selhání software	Technologické	2	4
		17	Zpronevěření aktiv	Lidské	2	3
		18	Zlomyslné kódy	Lidské	3	4
6	Podpůrný systém	19	Selhání software	Technologické	3	3
		20	Zlomyslné kódy	Technologické	2	3
7	Data	21	Neúmyslná modifikace	Lidské	5	3
		22	Vnější útoky	Lidské	3	5
		22	Krádež	Lidské	5	5
8	Know-how	23	Krádež	Lidské	4	5
9	Služby	24	Selhání komunikace	Lidské	3	5
		25	Epidemie	Přírodní	2	5
10	Elektronické faktury	26	Neúmyslná modifikace	Lidské	2	3
		27	Zpronevěření aktiv	Lidské	2	3
11	Energie	28	Výpadky sítě	Technické	2	3

Tabulka 4.5: Identifikace a ohodnocení hrozeb, určení zranitelnosti aktiv

4.5.4 Řízení rizik

Nejdříve bude zpracována matice zranitelnosti, kde budou zaneseny všechny důležité hodnoty z tabulek 4.2, 4.3, 4.4 a 4.5. Poté může být vytvořena matice rizik. U hodnot pravděpodobnosti vzniku hrozby a zranitelnosti aktiv se u hrozeb, které se opakují, musí určit střední hodnoty, abychom mohli pokračovat v dalších výpočtech.

Hrozba	**Suma hodnot**	**Počet výskytů**	**Střední hodnota**
Selhání hardware	14	4	3,50
Selhání software	4	2	2,00
Zastaralost hardware	10	3	3,34
Krádež	11	3	3,67
Zlomyslné kódy	5	2	2,50
Výpadky sítě	6	2	3,00
Požár	9	4	2,25
Vnější útoky	5	2	2,50
Zpronevěření aktiv	6	3	2,00
Neúmyslná modifikace	9	3	3,00
Selhání komunikace	3	1	3,00
Epidemie	2	1	2,00

Tabulka 4.6: Střední hodnota pravděpodobnosti vzniku hrozeb

Legenda tabulky 4.7:

- **A** - Hodnota aktiva
- **T** - Pravděpodobnost vzniku hrozby
- **V** - Zranitelnost aktiva

V tabulce 4.7 jsou uvedeny všechny důležité hodnoty, abychom mohli vypočítat míru rizika u určitých aktiv. Dle vzorce 3.8 bude vypočítána míra rizika (R) pro jednotlivá aktiva a bude sestavena matice rizik. Zaokrouhlení bude provedeno na celé číslo.

Dle tabulky A.7 lze jednotlivé rizika rozdělit do třech skupin. Mezi přijatelná rizika patří zpronevěření aktiv, mezi nepřijatelná krádež (zejména dat), třetím rizikem je pak selhání hardware a selhání komunikace. Těmto třem nejrizikovějším aspektům je třeba věnovat mimořádnou pozornost, nejdůležitější je například krádež dat. Mezi středně přijatelná patří i ostatní rizika.

V	Popis aktiva	Počítače	Notebooky	Serverovna	Tištěné faktury	IS SAP	Podpůrný systém	Data	Know-how	Služby	E-faktury	Energie
	A	4,67	4,00	5,00	3,67	5,00	4,33	5,00	4,67	5,00	3,67	5,00
Popis hrozby	**T**											
Selhání hardware	3,50	5,00	5,00	5,00								
Selhání software	2,00					4,00	3,00					
Zastaralost hardware	3,34	3,00	3,00	4,00								
Krádež aktiva	3,67		4,00					5,00	5,00			
Zlomyslné kódy	2,50					4,00	3,00					
Výpadky sítě	3,00			4,00								3,00
Vzniklý požár	2,25	5,00	5,00	5,00	5,00							
Možné vnější útoky	2,50			5,00				5,00				
Zpronevěření aktiv	2,00				3,00	3,00					3,00	
Neúmyslná modifikace	3,00				3,00			3,00			3,00	
Selhání komunikace	3,00									5,00		
Hrozba epidemie	2,00									5,00		

Tabulka 4.7: Matice zranitelnosti (V)

R	**Popis aktiva**	**Počítače**	**Notebooky**	**Serverovna**	**Tištěné faktury**	**IS SAP**	**Podpůrný systém**	**Data**	**Know-how**	**Služby**	**E-faktury**	**Energie**
	A	4,67	4,00	5,00	3,67	5,00	4,33	5,00	4,67	5,00	3,67	5,00
Popis hrozby	**T**											
Selhání hardware	3,50	82	70	88								
Selhání software	2,00					40	26					
Zastaralost hardware	3,34	47	40	67								
Krádež aktiva	3,67		59					92	86			
Zlomyslné kódy	2,50					50	33					
Výpadky sítě	3,00			60								45
Vzniklý požár	2,25	53	45	56	41							
Možné vnější útoky	2,50			63				63				
Zpronevěření aktiv	2,00				22	30					22	
Neúmyslná modifikace	3,00				33			45			33	
Selhání komunikace	3,00									75		
Hrozba epidemie	2,00									50		

Tabulka 4.8: Matice rizik (R)

5 Vlastní návrhy řešení

Na základě provedených analýz v předchozích kapitolách budou shrnuty jednotlivé analýzy a proveden návrh řešení. Tato kapitola pak bude završena metodou PERT.

Jedna z možností řešení bezpečnostní politiky je vytvoření nové bezpečnostní politiky za pomocí vlastních sil, což je levnější řešení, avšak nemusí odpovídat všem požadovaným standardům na ochranu společnosti. Podstatné je mít alespoň nějakou politiku nežli žádnou.

Druhá možnost je využití služeb specializované společnosti, která se touto problematikou už nějakou dobu zabývá a všechny nedostatky vytvoření bezpečností politiky vlastními silami může eliminovat. Přestože by to byla investice určitě vyšší než v prvním případě, byla by to investice jednorázová.,V dalším by bylo vhodné tuto úroveň minimálně udržovat, optimálně zvyšovat. Třetí možností je kombinace předchozích dvou možností, proto se tato varianta jeví lepší než první. V průběhu dalšího textu bude výsledek jednoznačnější než na začátku této kapitoly.

Principem tvorby bezpečnostní politiky je vytvoření nové dokumentace, z které budou vyplývat veškeré odpovědnosti osob, které jsou s bezpečnostní politikou nějakým způsobem svázány. S bezpečnostní politikou jsou logicky propojeni všichni zaměstnanci, kteří pracují s informačním systémem. Proto ji musí dodržovat všichni zaměstnanci a její plnění musí být kontrolováno pověřenými osobami, jako jsou vedoucí pracovníci. Pokud bude tedy bezpečnostní politika existovat, např. v papírové formě, a zaměstnanci budou proškoleni, podpisem stvrdí povinnost jejího dodržování a v případě bezpečnostního incidentu se již zaměstnanec nemůže vymlouvat na neznalost těchto rizik., principem je znalost různých rizik a možných situací, které mohou nastat v případě nějakého rizikového chování a předejít tak případnému nebezpečnému bezpečnostnímu incidentu.

Předmětem této kapitoly bude tvorba nové bezpečnostní politiky včetně ostatních doporučení.

5.1 Způsoby potlačení rizik

Způsoby potlačení rizik jsou součástí **řízení rizik**. Bezpečnostní politika ve společnosti je z obecného hlediska liberální. Ve svých pravidlech umožňuje realizovat téměř vše, výjimky jsou explicitně vyjmenované. Nějaká psaná pravidla v podniku sice existují, jsou uvedená ve smlouvě, například nevyzrazování informací, firemních dat (což nadále trvá i po opuštění společnosti po určitou dobu). Ale žádná dokumentace ohledně bezpečnostní

politiky neexistuje, což je problém. Pokud existují pravidla v mluvené formě, efekt z jejich dodržování je také téměř nulový. Na začátku stanovení takových pravidel nějaká efektivita může být na místě, ale časem opadne a vymizí. Proto by i tento nedostatek měl být odstraněn. Ze začátku se zde zaměříme na způsoby potlačení rizik.

Z předchozích analýz se tato práce zaměřila na několik rizik, kterým je potřeba věnovat určitá pozornost. Samozřejmě záleží na závažnosti rizika, což bylo vyhodnoceno. V tabulce 5.1 je uveden přehled rizik, způsob jejich potlačení.

Č	**Hrozba**	**Míra rizika**	**Způsob potlačení rizika**
1	Selhání hardware	Vysoká	Zadržení
2	Selhání software	Střední	Redukce
3	Zastaralost hardware	Střední	Redukce
4	Krádež	Střední	Zadržení
5	Zlomyslné kódy	Střední	Redukce
6	Výpadky sítě	Střední	Redukce
7	Požár	Střední	Transfer
8	Vnější útok	Střední	Redukce
9	Zpronevěření aktiv	Nízká	Redukce
10	Neúmyslná modifikace	Střední	Redukce
11	Selhání komunikace	Vysoká	Zadržení
12	Epidemie	Střední	Retence

Tabulka 5.1: Hranice přijatelnosti rizik

5.1.1 Selhání hardware

U selhání hardware se z hlediska vysokého rizika musí zamezit jeho výskytu, aby se minimalizovala jakákoliv způsobená škoda vyplývajícího z bezpečnostního incidentu. V případě hardware se musí postupovat velmi obezřetně od začátku nákupu hardware až po řešení případné údržby. V případě nákupu nového hardware, ať už se to týká počítačů nebo jen řezačky na dopisy (toto riziko lze napasovat na veškerý hardware v podniku), musí se vycházet již z osvědčených forem, které hardware dodávají. V prvním případě by v podniku měla fungovat IT skupina lidí, nebo, pokud se nejedná o velký podnik, může to být i jen jednotlivec (vedoucí - CIO), který bude mít na starosti veškerá aktiva a s tím spojená rizika, respektive celou bezpečnostní politiku. Součástí této politiky může být právě výběr hardware a pravidla podniku pro jeho nákup, proto to musí být osoba již vysoce kvalifikovaná. Pokud tuto osobu v podniku nemáme, musíme se rozhodnout, zda-li tuto osobu budeme najímat, nebo ponecháme současný stav, nebo budeme tento proces outsourcovat. Pokud jde o kvalitu včetně adekvátního rozvoje, druhá možnost se nedoporučuje.

Hlavní myšlenkou v nákupu hardware je vypracování seznamu třech až pěti dodavatelů, jejich vyhodnocení a na základě tohoto vyhodnocení či doporučení provést výběr optimálního dodavatele. Při vyhodnocování lze posuzovat hlediska jako je rychlost dodání,

úroveň servisu, délka opravy, způsob jednání, cenová politika. Lze najít více faktorů, které lze posuzovat a dle potřeb podniku lze stanovit i váhy dle preferencí podniku a stanovit tak vážené průměry. Ten dodavatel, který dostane nejvíce bodů, je zpravidla i vhodným kandidátem. V případě opakovaného porušení požadavku nebo jiného zásadního porušení by se dodavatel měl evidovat na černé listině a jeho služeb již v budoucnosti nevyužívat.

K dalším doporučením ohledně zadržení rizika je sestavení průběžných kontrol úklidu okolí hardware a čištění (servis) hardware. Vhodné by bylo umístit v kancelářích měřící přístroje vlhkosti. V tabulce 4.8 jsou kriticky ohrožena aktiva jako PC, notebooky a serverovna. Pokud se bude dodržovat správný servis u PC a notebooků, životnost hardware se dá podstatně prodloužit. Do serverovny může mít přístup jen kvalifikovaná IT osoba. Zde by měly být zajištěny veškeré bezpečnostní prvky, jako je požární systém, zaznamenávání činnosti na paměťové médium, dostatečná klimatizace a čistota.

5.1.2 Zastaralost hardware

Zastaralosti hardware se těžko předchází. Každý hardware má určitou životnost a pouze šetrné zacházení může životnost prodloužit. Největším nepřítelem hardware je teplo a prach, proto je vhodné zajistit na pracovišti čisté prostředí, a udržovat vhodné klimatizované prostředí.

Dost často se stává, že někteří zaměstnanci při odchodu z práce nevypínají svůj počítač. Dochází pak k tomu, že se hardware zbytečně opotřebovává, stárne a snižuje se tedy jeho životnost. i když tato skutečnost není přímo dokázána. S tím souvisí i zbytečná spotřeba elektrické energie zvyšující náklady podniku.

Běžná provozní doba PC je 8,5 hodiny, což za rok činí 2040 hodin. V praxi existují situace, že zaměstnanci svůj počítač nevypínají, počítač je v provozu i přes víkend, kdy v práci nikdo není. Po výsledné kalkulaci se v tomto případě jedná o provoz po dobu 8064 hodin za rok. V porovnání s prvním případem bude elektrická energie spotřebována a hardware opotřebovaný 4x rychleji oproti době při řádném dodržování vypínání počítačů po skončení pracovní doby.

5.1.3 Selhání software

Selhání software může být zapříčiněno nedostatečnými aktualizacemi programů (včetně stahování patchů). Dále neodborným zacházením s instalovanými programy, jedním z důvodů může být i možnost instalovat programy dle libosti zaměstnance. Redukce rizika tkví v zakázání neřízených instalací programů. Je to možné nastavit IT pracovníkem v operačním systému. Situaci lze ošetřit předpisem či dokumentací k povolení instalace nějakého programu, kdy na základě posouzení IT pracovníka bude program nainstalován. Zabrání se tak riziku instalace pirátských verzí programů, pak následných pokut z případných kontrol. Přestože kontroly chodí výjimečně, přesto riziko a vznik bezpečnostního incidentu existuje.

Navíc v případě instalace nadměrného množství programů se v operačním systému plní registry nadbytečnými daty, což zpomaluje PC. Je nutné neustále aktualizovat antivirové programy, které by měly být v porovnání s ostatními antiviry efektivní v případě zachycení

nějaké hrozby. Redukovat rizika v případě operačního systému lze eliminovat nákupem novější verze operačního systému. V našem případě je na většině PC nainstalován Windows XP, pro který končí podpora společnosti Microsoft, proto se postupně přechází na sytém Windows 7 nebo Windows 8.

5.1.4 Krádež aktiva

Krádež aktiva může být porovnávána z hledisek zásahu zaměstnance nebo cizí osoby. Pokud jde o zaměstnance, je to asi nejhorší způsob, který může nastat. Může totiž předat informace třetí straně, respektive předat know-how, vynést data konkurenci. Vždy jde o konkurenční boj mezi podniky. Záleží, jestli zaměstnanec způsobí škodu během pracovního poměru nebo až po skončení. V druhém případě záleží, jestli zaměstnanec rozvázal pracovní poměr přátelsky nebo nepřátelsky, kdy se pravděpodobnost krádeže aktiva zvyšuje.

Ve všech případech krádeže se musí veškerým možným bezpečnostním incidentům zabránit, a to dodatkem při podpisu smlouvy, kde jsou zahrnuty vysoké pokuty doprovázené soudním procesem. Toto pravidlo by mělo platit minimálně pět let po rozvázání pracovního poměru.

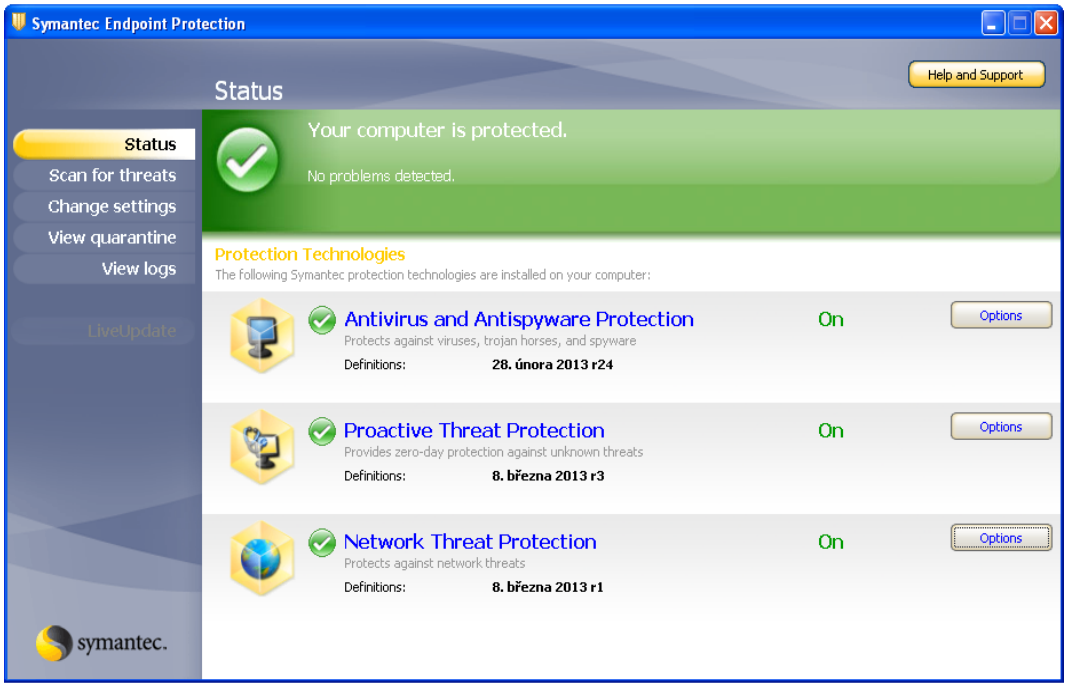
Zabránění krádeži aktiva cizí osobou lze zabránit pouze vymezením přístupu do kanceláří přes čipové karty, důsledným zavíráním dveří, nepuštěním cizích osob bez dozoru na místo pracoviště, nezveřejňováním obsahu práce zaměstnance na veřejnosti, kontrolou prostor kamerovým systémem, vhodnou ostrahou objektu a bezpečnostní ochranou proti vnějším útokům na počítačovou síť. Dalším důležitým faktorem je vhodná volba šifrování dat, která by měla být řešena na všech počítačích bez výjimky.

5.1.5 Zlomyslné útoky

Zlomyslnými útoky mohou být především útoky zvenčí, proto nelze podceňovat instalace efektivního antiviru. Firma používá antivir Norton Symantec. K tomu je třeba dodržovat základní pravidla práce s internetem, kdy by neměly být navštěvovány neznámé stránky, neprověřené odkazy apod. S tím souvisí restrikce přístupu na webové veřejné stránky, povolení by mělo fungovat jen na intranet, pouze vedoucí pracovníci by měli mít přístup na veřejný internet. Pokud mají tuto možnost všichni, pak by se činnost na webu měla kontrolovat.

Pokud podnik využívá vhodný antivirový program, je nutné provést benchmarking. To není složitá záležitost, na internetu lze nalézt benchmarking free antivirů jak je patrné z obrázku 5.2. Zde je vidět, že antivir disponuje ochranou před všemi útoky zlomyslných kódů a nevede si vůbec špatně v poměru cena/výkon. Určitě by se nějaký substitut našel v podobě antiviru číslo jedna na obrázku 5.2, ale rozdíl není tak markantní, aby to vedlo ke změně antivirového programu.

V souhrnu lze tvrdit, že antivir Norton Symantec by měl bezpečně uchránit počítače před škodlivými kódy. V případě redukce rizika je nutné zadokumentovat jak se chovat v případě „brouzdání“ po internetu, kdy omezit přístup z externích zdrojů, jako z USB



Obrázek 5.1: Symantec Endpoint Protection

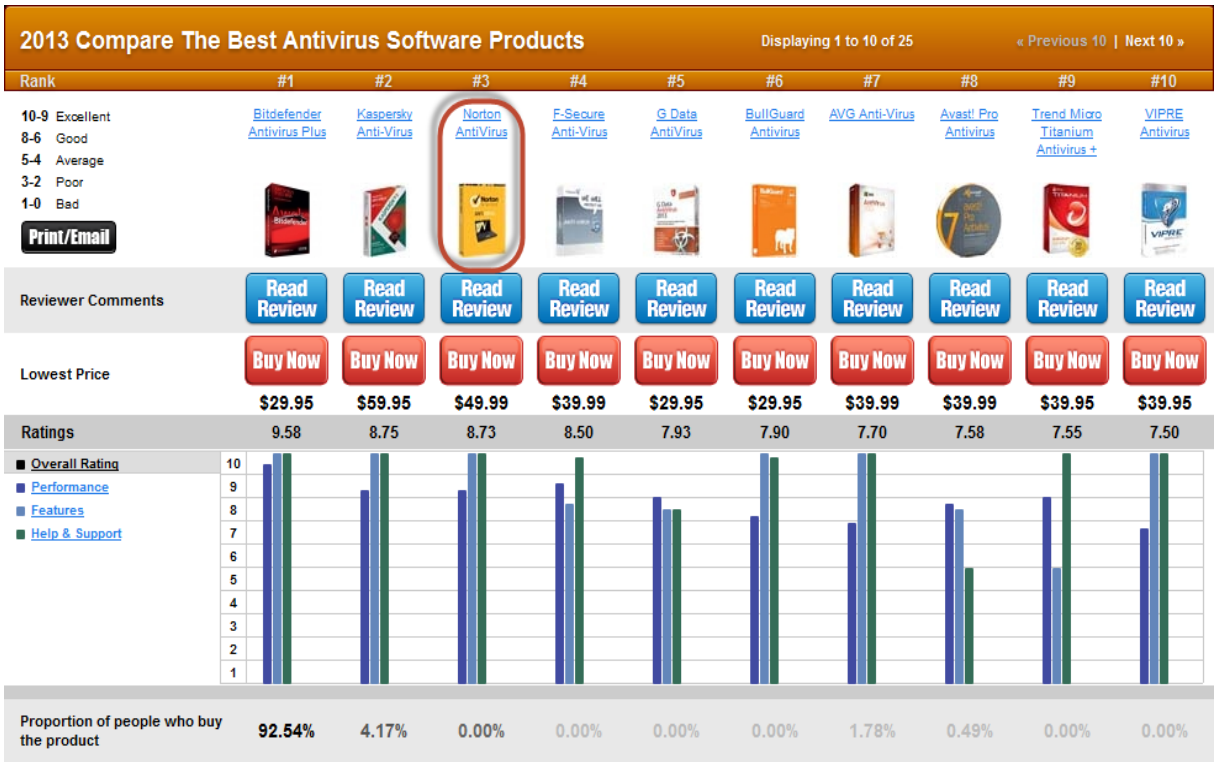
flash disků nebo jiných periferií, vše lze nastavit v administrátorském přístupu v operačním systému.

5.1.6 Výpadky sítě

Výpadky sítě mohou negativně ovlivnit činnost zaměstnanců v podniku. Ať už se jedná o výpadek elektrické energie nebo internetové sítě či intranetu, k redukci rizika ve všech případech je nutno provádět pravidelné kontroly hardware, mít sjednaný kvalitní servis v případě poruchy, případně mít vhodné záložní zdroje, které mohou riziko znatelně snížit. V případě internetu a intranetu by řešení mělo být předmětem činnosti IT pracovníků. Elektrická síť je v zodpovědnosti pronajímatele, proto si podnik musí být jistý, že správce budovy je schopen zajistit včasnou opravu v případě havárie, event. přepojení na záložní zdroje apod.

5.1.7 Vznik požáru

Riziko vzniku požáru není příliš vysoké, dodržují-li se stanovená pravidla při pobytu v budově, při práci na opravách různých zařízení apod. Riziko hrozí v případě možných zastaralých či neudržovaných zařízení např. v obslužných prostorách jako jsou např. kuchyňky.Proto je dobré, že jsou všude požární hlásiče a automatické hasící přístroje. Větší pozornost těmto bezpečnostním zařízením se musí věnovat v serverovně, včetně jejich pravidelné kontroly. Riziko vzniku požáru lze přenést na jinou, tedy pojišťovací společnost,



Obrázek 5.2: Benchmarking antivirů v roce 2013 (32)

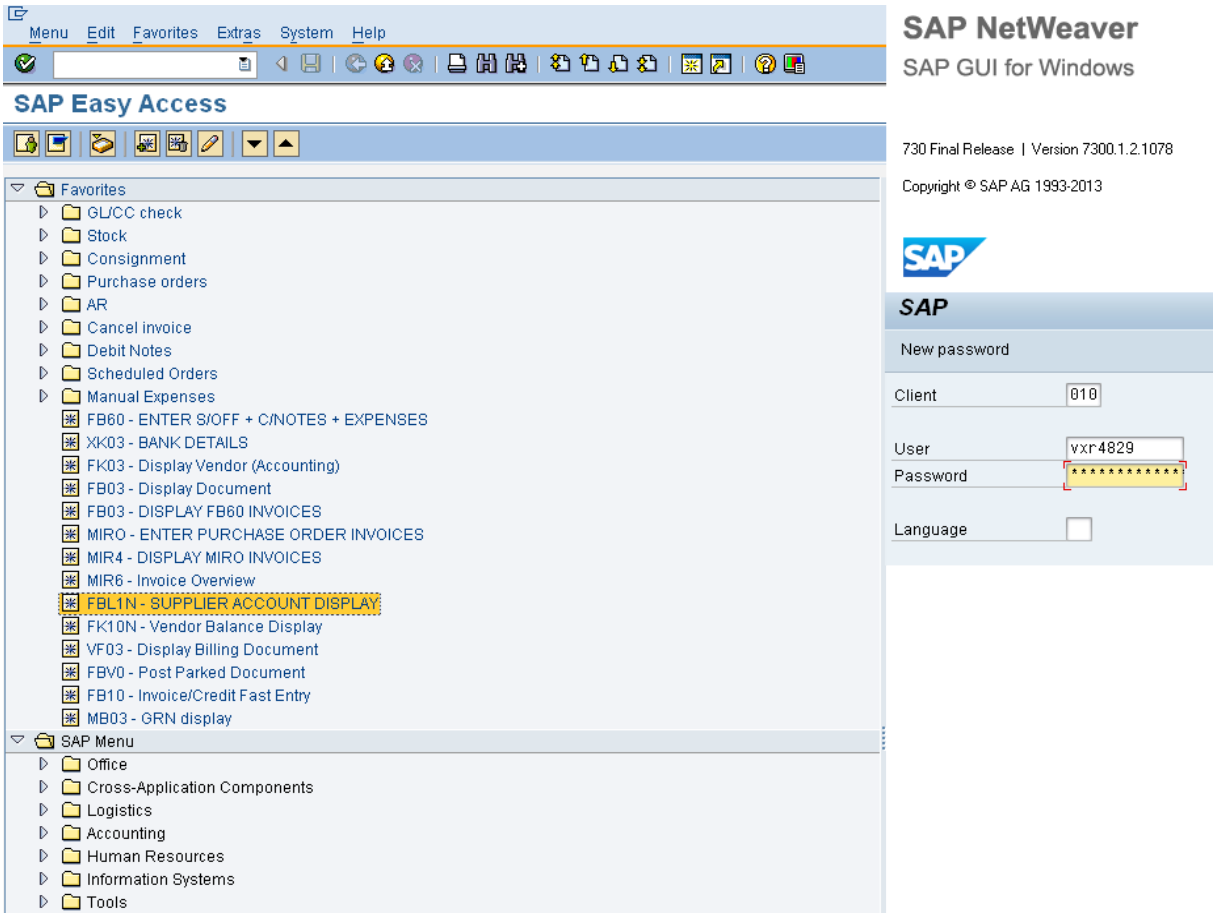
kdy v případě výhodného balíčku se lze komplexně pojistit i proti jiným rizikům.

5.1.8 Vnější útoky

Součástí antivirového programu Norton Symantec je firewall, základní firewall obsahuje i operační systém Windows. Firewall by měl ochránit aktiva podniku před vnějšími útoky. Investice do nějakého speciálního firewallu může být finančně náročná a je otázkou, zda by tato investice přinesla očekávaný užitek. Další pojistkou je i používaný Verizon, je ale na vzdáleném serveru mimo ČR.

Data jsou velmi důležitou součástí podniku. Pravidelný servis defragmentace a analýzy disků by měl zajistit rychlost pracování s daty, což je úkolem plánování IT pracovníků, lze nastavit i automaticky a předejít tak nechtěným výpadkům či pomalosti systémů.

Redukce rizika proti vnějším útokům je zajišťována školením pracovníků, mj. o zákazu vynášení či vyzrazení různých důležitých informací jako je třeba IP adresa. Je třeba pamatovat i na možnost vyzrazení citlivých informací při odesílání různých zpráv, screenshotů apod.



Obrázek 5.3: Produkční prostředí informačního systému SAP

5.1.9 Zpronevěření aktiv

V případě záměrné modifikace dat může dojít k odeslání peněžních prostředků na jiný účet, než na který bylo zamýšleno. Tento typ rizika zpronevěření aktiv však lze redukovat pomocí SOD[1] rozdělením pravomocí v týmu, myšleno ne ústní formou, ale samozřejmě písemnou a i zdokumentovanou, tedy kdo je za co zodpovědný, doplněné vzorovými podpisy. Pak by taková situace vzniku rizika neměla nastat, nenastane-li tato situace cíleně působením jednoho či skupiny zaměstnanců záměrně.Vznik tohoto bezpečnostního incidentu je předmětem trestné činnosti, pravděpodobnost vzniku rizika není vysoká.

Únik informací o dodavatelích a odběratelích může poškodit goodwill a image podniku, včetně vyzrazení know-how konkurenci. SOD tuto situaci ošetřuje, sice ne úplně, ale zaměstnanec ví pouze přesně to, co k danému druhu činnosti potřebuje. Proto by bylo i vhodné zamezit přístup zaměstnanci k datům, které nepotřebuje, což je opět odpovědnost IT pracovníka. Míra rizika zde není vysoká. Doporučuje se redukce rizika, protože zde existuje propojení hrozeb mezi ostatními riziky a speciálně SOD je uplatnitelné k redukci

[1]Segregation Of Duties

a zadržení rizik u ostatních aktiv.

Součástí zpronevěření aktiv je zneužití tisku dokumentů pro svou vlastní potřebu. S tímto bezpečnostním incidentem se setkal snad každý podnik. Tisk dokumentů pro svou vlastní potřebu je klasifikován jako krádež podnikových prostředků a zneužívání nákladů podniku. Zabránění tomuto incidentu není jednoduché, bylo by vhodné využití služeb nějakého sofistikovaného programu slouží- cího k redukci tohoto rizika.

5.1.10 Neúmyslná modifikace

Tolerance chybovosti je při prováděných procesech v podniku nulová, avšak lidský faktor není neomylný a chyby se v praxi vyskytují. Jedná se o neúmyslnou modifikaci dat, které vedou k pozdním nebo předčasným platbám, což může negativně ovlivnit image podniku (platební morálka) nebo cash flow z pohledu AP a z pohledu AR obráceně. Může dojít k platbě na špatně zadané bankovní detaily nebo na špatně nastaveného dodavatele nebo peníze nemusí dorazit vůbec při špatném zadání bankovních detailů odběratelem. Podnik by měl aplikovat SOD jako u zpronevěření aktiv.

V případě dodavatele se mohou vyskytovat ještě další problémy, jako jsou fiktivní změny bankovních detailů, v tomto případě je vhodné vytvořit dokumentaci, která tento problém ošetří ve smyslu dvojího potvrzení změny ze dvou zdrojů. Navíc je potřebné prověřovat správnost a úplnost údajů na fakturách pro zamezení případných falešných plateb.

V případě odběratele může nastat situace, že se pošle zboží, faktura, ale ta není ani po splatnosti uhrazena. To musí být ošetřeno dokumentací s doporučením dodavatele, který dodává odběrateli, jenž si u tohoto podniku zboží objednal, musí se vést i evidence podniků. Aby nedocházelo k častým chybám, je nutné veškeré postupy procesů zdokumentovat a zpřístupnit těm zaměstnancům, kteří je ke svému výkonu potřebují, je nutné je neustále aktualizovat a tyto aktualizace vhodně v dokumentu uvádět.

5.1.11 Selhání komunikace

Selhání komunikace může vést k totální devastaci podniku. Může nastat ve vnitřním a vnějším prostředí. Vnitřní prostředí se týká managementu, týmu a uvnitř týmu. Proto se musí management pečlivě věnovat výběru členů do týmu, umět tým motivovat, a to nejen finančně. Zaměstnanci v týmu by si měli rozumět a směřovat ke stejnému cíli. Do vnitřního prostředí patří komunikace mezi dodavateli a odběrateli na profesionální úrovni.

Základem pro dobré fungování komunikace je motivace lidí, otevřenost novým názorům a vyslechnutí každého názoru, pocit sounáležitosti s děním v podniku. Vhodnými se pak jeví např. různá neformální setkání mezi zaměstnanci a vedoucími pracovníky na různých teambuildincích apod.

Pokud bude zajištěno fungování vnitřního prostředí, mělo by fungovat i to vnější, pojištěné výkonnostními bonusy, na které si zaměstnanci velmi rychle zvyknou. Tyto aspekty je vhodné zadokumentovat do podnikových procesů a zaměstnaneckých smluv.

5.1.12 Epidemie

Míra rizika propuknutí epidemie, tedy nějaké nemoci v podniku existuje na střední úrovni. Největším rizikem, vzhledem k úrovni zdravotnictví v ČR, je snad jen propuknutí chřipkové epidemie, která každoročně ohrožuje jednotlivé kraje v České republice.

Jelikož se zde pracuje v „open space“ prostorech, což jsou obrovské otevřené prostory, kde nejsou oddělené místnosti, je vhodné toto riziko redukovat například příspěvkem na vakcíny proti chřipkám.Záleží samozřejmě na finanční situaci podniku, dále lze zavést tzv. sick days, což jsou dny, kdy člověk může zůstat doma bez nutnosti předložení neschopenky, a to aniž by přišel o mzdu. Redukuje se tím riziko šíření nemoci po celé budově, které by se díky klimatizaci a vlhkému prostředí dařilo. S tím souvisí další redukce rizika, a to pravidelný servis klimatizací, kde se choroboplodné zárodky usazují, zamezí se tím i možnému vzniku alergií u některých zaměstnanců.

5.2 Řešení bezpečnostní politiky

Po vytvoření dokumentace z předchozí kapitoly se doporučuje provést řešení bezpečnostní politiky dle standardů ISO/IEC skupiny 27000. Existují tři možnosti řešení, a to vytvoření varianty na základě vlastního řešení nebo využití služeb profesionálního podniku nebo kombinace obou předchozích návrhů. První řešení je sice méně nákladné, ale není zaručena efektivnost. Druhé řešení je vyhovující, ale nedává posuzovaném podniku stoprocentní kontrolu nad celkovou stránkou bezpečnosti IS a nelze flexibilně reagovat na nové vzniklé situace. Proto se třetí řešení jeví jako optimální. Podnik, který se touto problematikou už nějakou dobu na trhu zabývá, je Safetica Technologies se sídlem v Praze a pobočkou v Brně. Poskytuje podporu ve více než 50 zemích. Součástí případné spolupráce by byla SLA.

Řešení problematiky bezpečnostní politiky podnik zajišťuje ve dvou variantách, malá instalace a standardní instalace, kde druhá varianta je vhodná pro posuzovaný podnik.

5.2.1 Ochrana před selháním lidského faktoru

Předmětem této ochrany je řešení prevence před únikem dat (DLP[2]) z podniku. Podnik Safetica spravuje tok dat podle bezpečnostních pravidel tak, že pokud se bude někdo snažit tato pravidla obejít, podnik o takovéto akci bude ihned upozorněn. Nové soubory jsou chráněny ihned po vytvoření.

5.2.2 Prevence úniku dat

Pomocí Safetica Management Console (dále jen SMC) lze řídit řadu akcí, nastavení práv přístupu, ovládání bezpečné zóny, vyhodnocení různých analýz apod. Tento přístup

[2]Data Lost Prevention

k bezpečností politice je aplikovatelný nejen na stolních počítačích, ale i noteboocích, protože vše je ovládáno pomocí vzdáleného přístupu zabezpečeného šifrováním.

V případě bezpečnostního incidentu je podnik upozorněn a má možnost nahlédnout do zprávy, kde je uvedeno, co se dělo před, během a po útoku. Tyto výpisy lze pohodlně zobrazit nejen na vzdáleném počítači od místa bezpečnostního incidentu, ale i z mobilního přístroje, který má podporu přijímaní emailů.

5.2.3 Správa zařízení

V případě nepozornosti zaměstnance a ztráty notebooku nebo flash disku či jiného paměťového média je obsah chráněn silnou šifrou. Pokud zaměstnanec zapomene heslo k dešifrování obsahu média, neznamená, že je vše ztraceno, protože podnik bude vlastnit asymetrický klíč k jeho dešifraci a management bude schopen znovu data zpřístupnit.

Podnik Safetica řeší i problematiku kontroly nad přenosnými médii, konkrétně vytvoření bezpečných zón, kde může být nastaveno, jaká přenosná média v této zóně mohou být sdílena a která nikoliv. Něco podobného platí i pro nastavení části celé sítě, jako jsou tiskárny a jiná přenosná zařízení. Totéž platí i pro zákaz přístupu na média, která si přinese a připojí sám zaměstnanec k počítači nebo notebooku.

5.2.4 Šifrovaní dat

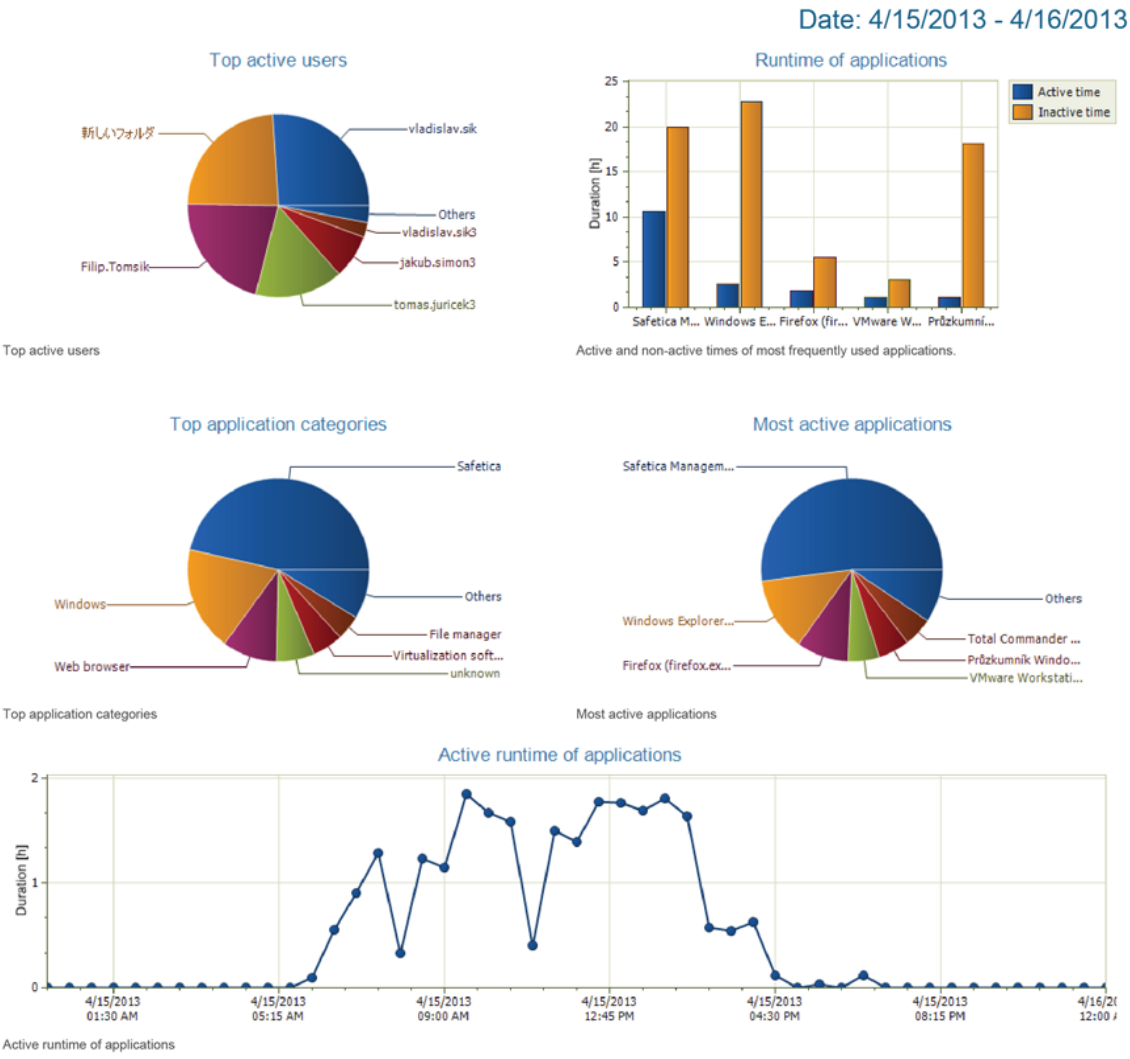
V případě počítačů, notebooků a přenosných podnikových médií budou data kódována silnou šifrou. Asymetrickou šifru bude mít k dispozici pouze management pro případ vzniku bezpečnostního incidentu.

Ochrana dat může být řešena i v případě komunikace s dodavateli a odběrateli, to však není třeba, protože ke vzniku incidentu by druhá strana musela vlastnit softwarové řešení podniku Safetica, navíc IBM Lotus Notes v případě emailové komunikace umožňuje šifrování, které zcela zamezuje nebo ztěžuje vznik takového incidentu.

5.2.5 Měření produktivity

V každé společnosti zaměstnanci mají nějaké přesčasy. Tyto přesčasy vznikají buď z důvodů nadměrné práce nebo rozptýlením zaměstnance od běžných pracovních úkolů. V druhém případě lze takovým incidentům zabránit měřením produktivity.

Měření produktivity sleduje veškeré aktivity zaměstnanců při práci na počítači nebo notebooku a poté vyhodnocuje. Management pak má vzdálený přístup k těmto výsledkům a může predikovat budoucí vznik bezpečnostního incidentu. Například v případě extrémní změny v chování zaměstnance je odeslán email osobě, která má zřízený vzdálený přístup k SMC. Některé podnikové procesy na základě těchto měření mohou být v budoucnu vylepšeny.



Obrázek 5.4: Ukázka měření produktivity zaměstnanců (33)

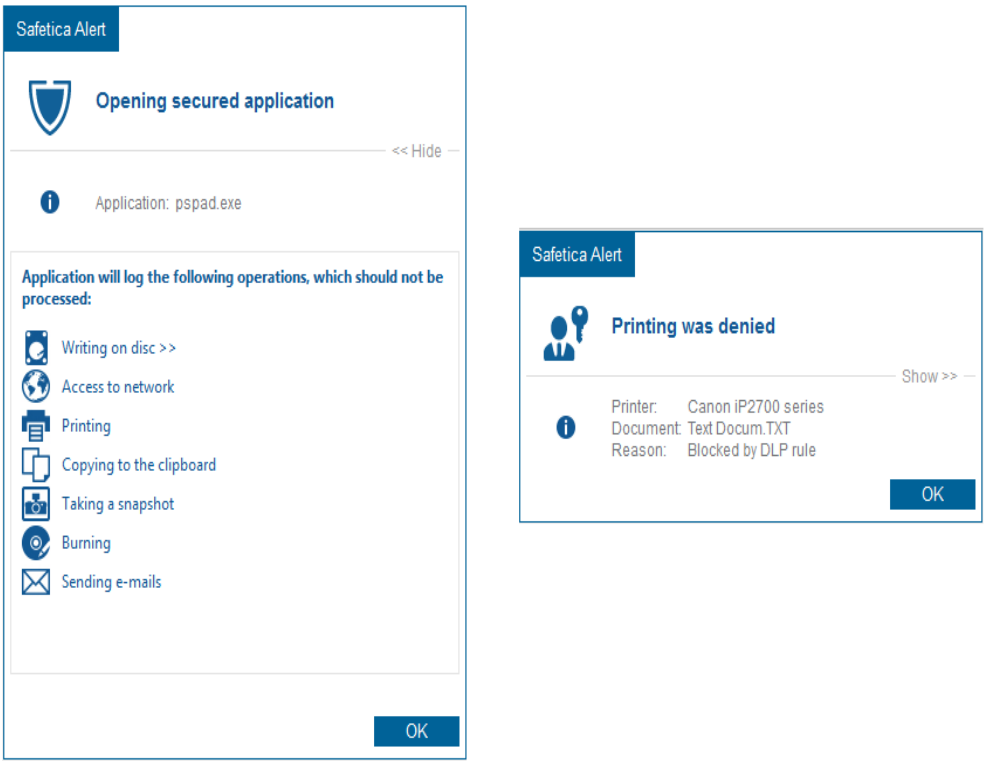
5.2.6 Záloha dat

V případě bezpečnostního incidentu krádeže hardware nebo celkového poškození bez možnosti znovuzískání dat, pokud by taková obnova dat byla příliš nákladná, je vhodné mít vhodně řešenou zálohu dat uloženou na pevném disku počítače nebo notebooku. Záloha dat je nyní řešena jen částečně, a to pouze pro email klienta IBM Lotus Notes a sdílené disky na severech. Bohužel to je málo. Obsah disku každého zaměstnance by měl být zálohován, optimálně jednou denně, protože se na něm nacházejí hodnotná data. Každý zaměstnanec by měl vymezenou kvótu pro zálohování dat, která by byla propojená se složkou na disku v počítači nebo notebooku. V případě bezpečnostního incidentu by mohla být data obnovena.

5.2.7 Blokování aktivity

Jak již bylo uvedeno v předchozích podkapitolách, podnik má možnost zablokovat přístup na určité vymezené webové stránky, přístup do aplikací a pro vyhodnocení má k dispozici reporty uživatelské aktivity. Lze tím zvýšit produktivitu všech zaměstnanců až o 30-40 %. V případě přístupu na webové stránky lze filtrovat přístup jen na ty internetové stránky, které souvisí s prací zaměstnanců, vše může být řízeno opět z SMC.

Jeden z důležitých bodů této podkapitoly je řízení nákladů na tisk. Výdaje na toner, servis zařízení včetně výdajů za papíry hrají neméně důležitou roli v nákladech podniku. V každé společnosti se takové bezpečnostní incidenty vyskytují, že zaměstnanci bez povolení provádějí tisk na podnikové papíry pro svou osobní spotřebu. Jedná se o součást rizika zpronevěření aktiv. Proto musí být i v tomto ohledu učiněno opatření blokováním možnosti tohoto neoprávněného využití firemních prostředků, i když je to obtížné a ne vždy musí přinést očekávaný efekt.



Obrázek 5.5: Ukázka blokování aktivity (34)

Software sice umí nastavit kvóty, výjimky a stanovení tisknutelných dokumentů. Umí i nastavení barevného nebo černobílého tisku, dále výběr aplikací, které mohou tisk využívat. Toto řešení nemusí být efektivní proto, že je třeba zabránit tisku jiných než podnikových dokumentů a tuto situaci software nedovede vyhodnotit, neboť např. každá faktura je jiná. Možností je tedy kombinace ostatních nastavení tohoto software blokování aktivity, ochrany dat a pak následné náhodné kontroly podezřelých dokumentů.

5.2.8 Chief Information Officer

Analyzovaný podnik by měl najmout vedoucího podnikové informatiky (CIO), který by byl zodpovědný za všechny bezpečnostní incidenty, které by v podniku nastaly. Z hlediska bezpečnostní politiky by vypracoval registr rizik jak je uvedeno v podkapitole 3.7.6, na základě kterého by mohl vypracovat seznam, jak se chovat i v případě vypuknutí bezpečnostních incidentů.

Hlavní úloha by byla řízení rizik v podniku a s tím spojené jejich potlačení, tedy vypracování podrobného plánu na základě zpracované kapitoly 4.5 a podkapitoly 5.1 spojené s využitím služeb společnosti Safetica Technologies, jako je řízení veškerého průběhu, vyhodnocování reportů, tvorby nápravných řešení (úzká spolupráce s managementem ostatních oddělení), nastavování bezpečnostních prvků v souladu s pravidly bezpečnostní politiky a mnoha dalších. Kombinace těchto řešení by vedla k optimálnímu řízení bezpečnostní politiky v posuzované společnosti. K dalším úkolům by patřila interní IT podpora místo externí podpory IT podniku, kde by se ušetřily dodatečné náklady za outsourcování IT procesů. Služby zaměstnancům by vzrostly na vyšší úroveň, zároveň by se zlepšila i celodenní podpora, proto se jeví nábor CIO optimálním řešením.

Nábor tohoto zaměstnance by zajišťovalo HR oddělení, které by mělo za úkol vybrat zkušeného a schopného kandidáta, který má alespoň 5 let zkušeností v oboru. V případě tvorby a implementace bezpečnostní politiky by veškeré aspekty byly konzultovány mezi CIO a agentem změny, což je management jednotlivých týmů, jak je uvedeno v kapitole 4.4. Podstatnou součástí smlouvy s IT manažerem by byla SLA, na základě kterého by podniku měly být poskytnuty ty nejlepší služby.

5.2.9 Bezpečnostní incidenty

Na základě výskytu rizik v podniku existuje pravděpodobnost vzniku bezpečnostních incidentů, které je nutno kontrolovat a přistupovat k nim takovým způsobem, aby jakýkoliv dopad na aktiva v podniku byl minimální. Jejich řízení bude mít na starosti IT manažer. Jeho úkolem je zajistit u všech bezpečnostních incidentů, co se stalo před, během a po vzniku incidentu a vše řádně zaprotokolovat, což je nutnou součástí bezpečnostní politiky. V případě vzniku bezpečnostního incidentu zaviněného zaměstnancem podniku musí být provedeno šetření obsahující popis jeho postihu. Postih bude vyhodnocený na základě závažnosti incidentu a dopadu na hodnotu aktiv (může přijít o veškeré finanční bonusy nebo dokonce i o zaměstnání z důvodu hrubého porušení pracovní kázně).

Mezi bezpečnostní incidenty patří:

- **Poškození hardware** - ať již opotřebením nebo zaviněním třetí osobou, CIO musí zajistit okamžitou nápravu. Tento bezpečnostní incident lze řešit pomocí udržování několika základních hardwarových součástek nebo sestav na skladě a v případě incidentu ihned provést odborný zásah. Pokud by došlo ke kritickému poškození celého zařízení, tak ihned provést výměnu. Pokud se nejednalo o periferii, ale například PC, tak obnovit zálohu dat aby nebyla přerušena činnost zaměstnance na dlouhou dobu.

- **Pád sítě** - kontrola serverovny, pokud není problém na straně podniku v Brně, tak neprodleně kontaktovat IT podporu v Německu a společně problém vyřešit.
- **Neautorizovaný vstup do prostor** - vstup cizí osoby na pracoviště nebo zaměstnance do prostor, kam nemá přístup. V případě vstupu cizí osoby na pracoviště bude daná osoba co nejdříve vyvedena ven z prostor podniku, v případě zaměstnance je daná osoba vyvedena ven z objektu a provedeno šetření.
- **Pořizování snímků na pracovišti** - dnes již téměř každý mobilní telefon disponuje fotografickým zařízením. Je zakázáno fotografování prostor podniku včetně jakýchkoliv aktiv, které by se mohly zneužít. Otázkou je, které takové incidenty se podaří odhalit. V případě odhalení bude provedena kontrola zařízení, případný materiál smazán a provedeno šetření.
- **Ztráta notebooku** - v případě šifrování pomocí Safetica siftware by data neměla být ohrožena před zneužitím. Nahlásit krádež policii ČR, nahlásit sériová čísla nejen policii, ale i výrobci. Nutno zahájit šetření se zaměstnancem. Jelikož zaměstnanec nemá podepsanou hmotnou zodpovědnost, nehradí ztrátu, která vznikla firmě.
- **Pád IS SAP** - okamžité kontaktování IT podpory v Německu, která musí provést nápravu, aby zaměstnanci mohli pokračovat ve své činnosti.
- **Pád software** - zjištění příčiny pádu software a jeho okamžitá náprava, v případě nutnosti jeho celá přeinstalace.
- **Krádež dat** - ve většině případech nebývá vznik tohoto bezpečnostního incidentu firmou odhalen. Pokud je tento incident odhalen, je okamžitě zahájeno šetření se zaměstnancem a vyčísleny škody úniku dat.
- **Neúmyslná modifikace dat** - chybovost zaměstnanců v podniku, kdy nedopatřením dochází ke změně dat tak, než tomu bylo původně vědomě zamýšleno. Dojde k upozornění zaměstnance, v případě neustálého opakování trénink.
- **Úmyslná modifikace dat** - cílené chování zaměstnance za účelem poškození společnosti. Proti zaměstnanci bude vedeno řízení.
- **Vnější útok** - útok cizí osoby, který se snaží poškodit aktiva podniku. Obnovit původní software nebo web ze zálohy, vyčistit soubory od škodlivého kódu a změnit hesla do administrace, posoudit vhodnost dosavadního firewallu.
- **Výpadek energie** - neprodlený kontakt správce budovy s požadavkem na okamžitou nápravu vzniklé situace.

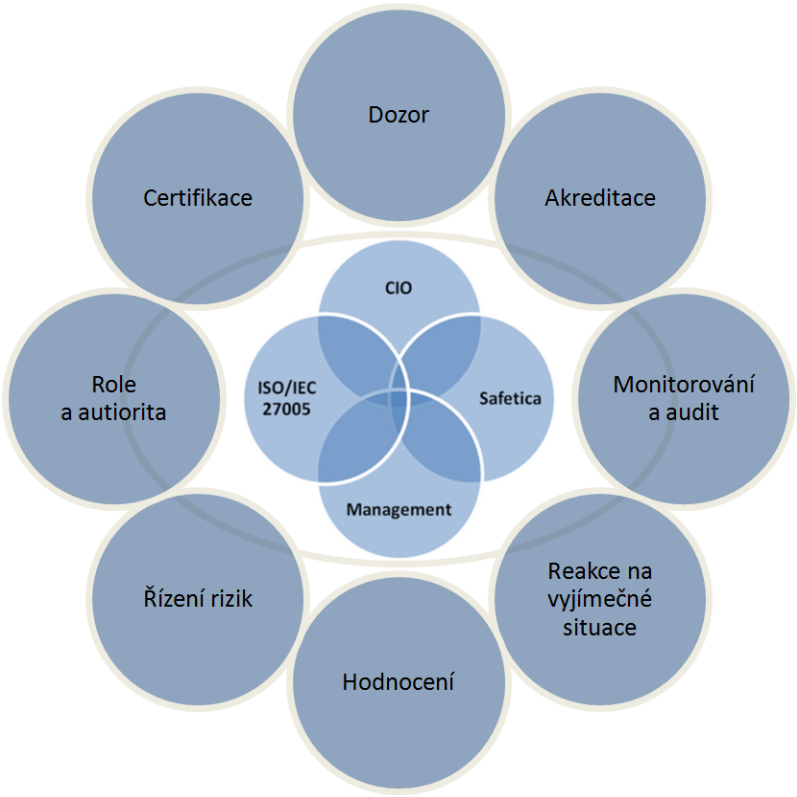
Pro vedoucího pracovníka v oblasti IT je velmi důležité flexibilně řešit bezpečnostní incidenty ihned po jejich odhalení. Jakékoliv prodlení v jejich řešení může způsobit vznik nákladů, proto je zde důležitá existence interních IT zaměstnanců.

5.2.10 Distribuce bezpečnostní politiky

Vychází z kapitoly 4.4. Vedoucí pracovník v oblasti IT za podpory agentů změn bude šířit informace ohledně bezpečnostní politiky pomocí emailů, nástěnek, školení a budoucích e-learningových školení formou testů. Cílem této distribuce je vštěpování pravidel všem zaměstnancům a v případě nových pravidel nebo jejich změny provést okamžitou implementaci.

5.2.11 Shrnutí bezpečnostní politiky

Na základě obrázku 5.6 lze řešení bezpečnostní politiky shrnout v několika bodech postavených na čtyřech hlavních pilířích, což je CIO, který bude má za úkol řízení podstatné části bezpečnostní politiky za podpory managementu, tedy agentů změn. Podpora fungování bezpečnostní politiky je zajištěna softwarem Safetica dle standardů ISO/IEC série 27000, tedy zahrnující i ISO/IEC série 27005 a mnoho dalších bezpečnostních standardů.



Obrázek 5.6: Řešení bezpečnostní politiky

- **Dozor** - je zajištěn CIO a managementem, obě dvě skupiny spolupracují, přičemž management má za úkol dohlížet na dodržování pravidel bezpečnostní politiky a v případě odhalení vzniku bezpečnostního incidentu neprodleně nahlásit CIO, který má za

úkol udržovat a aktualizovat bezpečnostní politiku a dohlížet na globální dodržování bezpečnostní politiky za podpory managementu.

- **Certifikace** - bezpečnostní politika je v souladu se standardem ISO/IEC 27005, tedy ohodnocování aktiv a rizik v podniku, a s tím následné dodržování pravidel bezpečnostní politiky. Certifikace je důkazem bezpečnosti IS.
- **Akreditace** - jako akreditační autorita je v tomto případě chápán podnik Safetica Technologies, která posuzovanému podniku udělí licenci k používání softwarového řešení bezpečnostní politiky v souladu s mezinárodními standardy.
- **Monitorování a audit** - pomocí software Safetica bude veškerou situaci ohledně bezpečnostní politiky a její dodržování monitorovat CIO, z následných analýz vyvozovat důsledky a případná opatření. Mezi monitorování situace ohledně bezpečnostní politiky patří i fyzická kontrola pracoviště, jinými slovy dodržování definovaných pravidel (například dodržení platnosti nebo změny hesla po prvním přihlášení, kontrola ostrahy objektu, přítomnost neautorizovaných osob ve vymezených prostorách apod.)
- **Reakce na vyjímečné situace** - sestavuje a řídí CIO na základě seznamu bezpečnostních incidentů, které budou velmi detailně rozepsány včetně procesních postupů krok za krokem, jak v dané situaci postupovat.
- **Hodnocení** - vychází z monitorování a auditu bezpečnosti IS/ICT, na základě kterého je pak v případě nedostatků bezpečnostní politika modifikována. Zodpovědná osoba je CIO, proces by měl být prováděn v pravidelných intervalech.
- **Řízení rizik** - zodpovědná osoba je CIO, kde jsou za podpory managementu ohodnocena aktiva, následně i z nich vyplývající rizika (matice rizik). Nakonec může být sestaven seznam bezpečnostních incidentů, které musí být dopodrobna rozepsány.
- **Role a autorita** - definice rozsahu zodpovědnosti managementu a CIO ohledně bezpečnostní politiky, obsahující i varianty postihu v případě porušení pravidel bezpečnostní politiky. Úzce souvisí s dozorem.

5.3 Odhad trvání implementace bezpečnostní politiky

Odhad trvání projektu bude sestaven pomocí stochastické metody PERT. Aby mohla být tato metoda využita, nejdříve musí být stanoveny a popsány jednotlivé uzly a činnosti, u kterých bude určen optimistický a pesimistický odhad, z toho očekávané trvání činností v časových jednotkách. Výpočty a výsledky celé metody pak budou zobrazeny v grafu.

5.3.1 Jednotlivé dílčí činnosti projektu

Nyní následuje krátký popis jednotlivých dílčích činností, z kterých budou vycházet výpočty pro další kroky stochastické metody PERT.

5.3.1.1 Nábor CIO

Proces náboru vedoucího IT pracovníka za účelem převzetí zodpovědnosti v IT oblasti a z pohledu tohoto projektu vedení a správu bezpečnostní politiky. Z časového hlediska bude tento proces trvat delší dobu než jeden den, protože nejprve bude muset HR oddělení vystavit inzeráty, absolvovat pohovory, při výběru bude participovat i management podniku. Po úspěšném ukončení náboru CIO již může spolupracovat na implementaci bezpečnostní politiky.

5.3.1.2 Konzultace ohledně náboru CIO

Konzultace agentů změn s HR oddělením ohledně náboru vhodného vedoucího pracovníka v IT oblasti.

5.3.1.3 Výběr dodavatele softwarového řešení bezpečnostní politiky

Průzkum nabídky trhu a sestavení seznamu možných kandidátů na dodavatele softwarového řešení bezpečnostní politiky (z veliké části zapojen ředitel podniku). Důležitými faktory je kvalitní monitoring činností ohledně IS a kvalitní poradenství v případě tvorby a udržování interní bezpečnostní politiky v podniku. V tomto případě všechny požadavky splňuje společnost Safetica Technologies. V případě úspěšného výběru dodavatele následuje podpis kontraktu a platba za poskytnuté licence, popřípadě služby.

5.3.1.4 Konzultace s CIO ohledně výběru dodavatele

Vedoucí pracovník v oblasti IT zrekapituluje veškeré faktory výběru dodavatele software bezpečnostní politiky.

5.3.1.5 Nevyhovující dodavatel

Úzce souvisí s předchozí činností, kdy v případě nevyhovujícího seznamu možných dodavatelů softwarového řešení bezpečnostní politiky se proces výběru dodavatele vrací zpět do předchozího bodu. Patří sem i souvztažná dílčí činnost zadokumentování nevyhovujících dodavatelů, následně pak přesun do bodu, z kterého vychází dílčí činnost výběru dodavatele.

5.3.1.6 Analýza aktiv a rizik s pomocí agentů změn

Tato činnost je náročnější z hlediska obsahu. Vychází z kapitoly 4.5, kde je potřeba nejdříve identifikovat aktiva (hmotný, nehmotný a finanční majetek) a ohodnotit aktiva. Dále provést analýzu hrozeb, z kterých budou vyselektovány rizikovější varianty a následně řízeny na základě vyhodnocení matice rizik za účelem předejití vzniku bezpečnostního incidentu v podniku. Smyslem je vypracování návrhů způsobů potlačení rizik, jejich seznam je uveden v kapitole 5.1. Jde o interní záležitosti bezpečnostní politiky, společnost Safetica Technologies by softwarovým řešením bezpečnostní politiky celou podnikovou bezpečnostní

politiku podporovala a upevňovala svou pozici ve společnosti k efektivnímu fungování IS a jeho okolí. Agenty změn je v tomto případě management jednotlivých týmů ve společnosti.

5.3.1.7 Analýza aktiv a rizik s pomocí CIO

Zcela navazuje na předchozí činnost, avšak tato činnost je podporována ze strany vedoucího pracovníka v oblasti IT.

5.3.1.8 Konzultace analýzy aktiv a rizik

Využití poradenských služeb dodavatele softwarového řešení bezpečnostní politiky v případě vlastní tvorby interní bezpečnostní politiky z důvodu zajištění integrace.

5.3.1.9 Implementace softwarového řešení bezpečnostní politiky

Fyzické nahrání softwarového řešení bezpečnostní politiky do počítačů a notebooků společnosti, propojení se sítí a servery. Test všech funkcí a vzdáleného přístupu. V případě funkčnosti všech prvků se považuje tato činnost za splněnou.

5.3.1.10 Konzultace dodavatele a CIO

Konzultace dodavatele softwarového řešení bezpečností politiky s CIO v souladu seznamu aktiv a řízení rizik. V podstatě se jedná o oddělení zdokukemtované interní bezpečnostní politiky od softwarového řešení, tedy vymezení toho, co bude obsahem softwarového řešení a následné sladění s interním řešením bezpečnostní politiky. Obě dokumentace pak budou spojeny dohromady.

5.3.1.11 Vytvoření seznamu aktiv a rizik

Vytvoření dokumentace spojující všechny aspekty bezpečnostní politiky na základě provedených analýz. Zahrnuta tvorba CIO včetně seznamu rizik (doplněné ostatními zaměstnanci podniku a doporučeními dodavatele software). CIO by měl mít hlavní slovo a podíl na tvorbě.

5.3.1.12 Vytvoření seznamu bezpečnostních incidentů

Hlavní tvorba dokumentace vedoucím pracovníkem v oblasti IT a s tím spojená i zodpovědnost. Podklad pro tvorbu bude seznam potlačení rizik.

5.3.1.13 Konzultace vhodnosti seznamu bezpečnostních incidentů

Poradenská činnost dodavatele softwarového řešení bezpečnostní politiky, tedy revize vhodnosti dokumentace seznamu bezpečnostních incidentů vycházejících ze seznamu potlačení rizik, jak jim předcházet a jak se v takovém případě chovat, kdo je za kterou část zodpovědný a jak popřípadě procházet bezpečnostním auditem.

5.3.1.14 Školení CIO na softwarové řešení bezpečnostní politiky

Provádění školení vedoucího pracovníka v oblasti IT na nově implementovaný software bezpečnostní politiky. Jde o školení na hlavní činnosti, tedy jak s takovým softwarem zacházet, jak provádět monitoring a správně vyhodnocovat získané analýzy.

5.3.1.15 Učení se všem funkcím softwarového řešení bezpečnostní politiky

Po provedeném školení se vedoucí pracovník v oblasti IT zaměří na všechny dostupné funkce software a získání tak všech vědomostí, jak se softwarem zacházet. Koncovým produktem této činnosti bude vytvoření podrobného manuálu pro interní potřeby podniku.

5.3.1.16 Tvorba bezpečnostní politiky

Spojení všech dosavadních nabytých dokumentací ohledně interní politiky a softwarového řešení bezpečnostní politiky (včetně manuálu) do jednoho hlavního dokumentu, který bude pravidelně (na základě stanoveného časového intervalu) aktualizován vedoucím pracovníkem v oblasti IT. Tento dokument se stane hlavní součástí dokumentace podnikových procesů a popřípadě pro potřeby externího bezpečnostního auditu.

5.3.1.17 Školení agentů změn

Školení ohledně bezpečnostní politiky vedené vedoucím pracovníkem v oblasti IT. Školenými osobami budou jen vedoucí pracovníci jednotlivých oddělení, kteří budou prováděné změny prosazovat ve svých týmech, za které jsou odpovědní. Vedoucí pracovník v oblasti IT bude kontrolovat dodržování bezpečnostní politiky a případné nedostatky konzultovat s vedoucími pracovníky daných týmů.

5.3.1.18 Školení ostatních zaměstnanců

Školení všech zaměstnanců na bezpečnostní politiku, předání všech doporučení a pravidel, včetně vysvětlení odpovědnosti, aby se zamezilo vzniku bezpečnostního incidentu. Nakonec všechny zaměstnance nechat podepsat dokumentaci o absolvování školení.

5.3.1.19 Identifikace agentů změn

Vymezení seznamu agentů změn, což bude management jednotlivých týmů. Na základě meetingu se sestaví dokumentace veškerých kompetencí managementu včetně implementace těchto pravomocí do kompetencí agentů změn. Na základě vytvořené dokumentace budou mít jasně vymezeno, co mohou a co ne.

5.3.1.20 Implementace bezpečnostní politiky

Zavedení bezpečnostní politiky v podniku. Jedná se tedy o první ostré spuštění monitorování a vyhodnocování analýz a uvedení interní bezpečnostní politiky v platnost. Součástí

této činnosti je i naplánování distribuce bezpečnostní politiky řízené vedoucím pracovníkem v oblasti IT. Tato distribuce bude mít formu pravidelných upozorňovacích emailů (jak se chovat, aby se zabránilo vzniku bezpečnostního incidentu doprovázených obrázky), nástěnkami s pravidly a upozorněními, pravidelnými školeními (stanovené na základě pravidelných časových intervalů, domluvených mezi CIO a agenty změn). Pozdějším plánem by mohlo být tvorba e-learningového školení formou testů, kde by zaměstnanci potvrdili i svoji uvědomělost pravidel bezpečnostní politiky a následků v případě jejich porušování.

5.3.2 Očekávané trvání činností projektu

Jednotlivé činnosti je nutno časově ohodnotit v hodinách (pracovní). Nejdříve je nutno stanovit *optimistický odhad trvání činnosti (a)*, *nejpravděpodobnější odhad trvání činnosti (m)* a *pesimistický odhad trvání činnosti (b)*. Jednotlivé činnosti budou časově ohodnoceny na základě odborného odhadu. Z těchto hodnot pak bude vypočítána střední hodnota *očekávané trvání činnosti* (t_c) na základě vzorce 3.3.

I	J	Činnost	a	m	b	t_c
0	1	Identifikace agentů změn	1,00	2,00	3,00	**2,00**
0	2	Nábor CIO	4,00	5,00	6,00	**5,00**
0	3	Výběr dodavatele BP	2,00	2,50	3,00	**2,50**
1	5	Analýza aktiv a rizik změn	6,00	7,00	8,00	**7,00**
1	2	Konzultace ohledně náboru CIO	0,25	0,50	0,75	**0,50**
2	5	Analýza aktiv a rizik dle CIO	2,00	3,00	4,00	**3,00**
2	3	Konzultace s CIO ohledně výběru dodavatele	0,25	0,50	0,75	**0,50**
3	4	Nevyhovující dodavatel BP	0,00	0,00	0,00	**0,00**
3	5	Konzultace analýzy aktiv a rizik	0,50	1,00	1,50	**1,00**
3	6	Implementace softwarového řešení BP	4,00	4,50	5,00	**4,50**
4	0	Nevyhovující dodavatel BP	0,00	0,00	0,00	**0,00**
5	7	Vytvoření seznamu aktiv a rizik	1,00	1,50	2,00	**1,50**
6	8	Konzultace ohledně seznamu BI	0,50	1,00	1,50	**1,00**
6	9	Školení CIO na softwarové řešení BP	2,00	3,00	4,00	**3,00**
7	6	Konzultace softwarového řešení BP s CIO	0,50	1,00	1,50	**1,00**
7	8	Tvorba seznamu bezpečnostních incidentů	1,50	2,50	3,50	**2,50**
7	11	Tvorba bezpečnostní politiky	6,00	7,00	8,00	**7,00**
8	9	Učení se všem funkcím softwarového řešení BP	4,00	5,50	7,00	**5,50**
9	10	Školení agentů změn prostřednictvím CIO	0,50	1,00	1,50	**1,00**
11	10	Školení zaměstnanců prostřednictvím CIO	2,00	2,50	3,00	**2,50**
10	12	Implementace bezpečnostní politiky	8,00	9,00	10,00	**9,00**

Tabulka 5.2: Očekávané trvání činností ve dnech

Na základě výpočtu očekávaného trvání činností lze pokračovat v dalších výpočtech vedoucích k výpočtu rozptylu trvání jednotlivých dílčích činností. Na základě tabulky 5.2

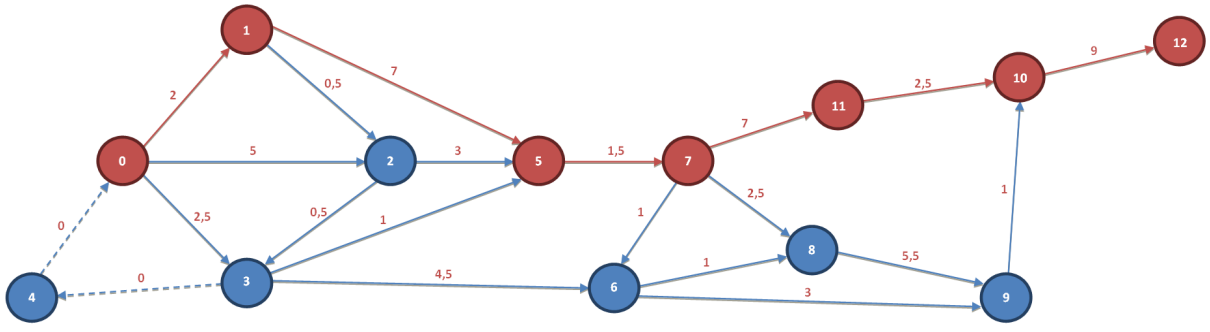
je možné sestavit základní obrázek grafu PERT, sestavený v příloze na obrázku A.7. Jakmile je graf PERT sestaven a jednotlivé činnosti ohodnoceny, je to výchozí bod k tomu, aby mohly být určeny kritické cesty v grafu, což umožňuje přiblížit pravděpodobný čas trvání projektu, na které činnosti se hlavně zaměřit, aby mohl být projekt úspěšný.

Jednotlivé činnosti mají různou délku trvání, z toho lze logicky usoudit, že rozptyl bude nabývat větších hodnot u činností, které mají vysoký počet pracovních hodin. Nejvíce má implementace bezpečnostní politiky, což je poslední článek v grafu metody PERT. Pokud bude uveden příklad činnosti výběru dodavatele bezpečnostní politiky z bodu 0 do bodu 3, předpokládá se, že tato činnost na základě předchozích výpočtů bude trvat 2,5 pracovních dní. Nyní, na základě metody PERT musí být vypočteny hodnoty jako nejdříve *možný začátek činnosti (MZ)*, *nejdříve možný konec činnosti (MK)* a *nejpozději přípustný konec činnosti (PK)*, *nejdříve přípustný začátek činnosti (PZ)*. Tyto hodnoty budou vypočítány na základě vzorců uvedených v kapitole 3.5.1.

Rozdíl mezi nejdříve přípustným začátkem (PZ) a nejdříve možným začátkem činnosti (MZ) je pak *časová rezerva (ČR)*, která udává počet volných nevyčerpaných pracovních hodin, které má podnik k dispozici. Jedná se o nekritické činnosti, u kterých podnik může prodlužovat nebo zkracovat dobu trvání, aniž by to ohrozilo celkovou dobu trvání celého projektu. Pokud by se tato rezerva vyčerpala a byla by nulová, pak by se z toho stala kritická činnost. Po určení kritických cest v grafu pak bude následně vypočítaný *rozptyl* $(D(t_c))$ u každé činnosti (směrodatná odchylka je odmocnina z rozptylu, pro výpočet je zvolen rozptyl), který je nezbytný pro určení pravděpodobnosti dodržení plánovaných termínů ukončení projektu.

Na základě tabulky 5.3 lze sestrojit graf kritické cesty, jak je uvedeno na obrázku 5.7 nebo ve zvětšené podobě, v příloze na obrázku A.8 . Kde je v tabulce výsledek časové rezervy nula pracovních dnů, jedná se kritickou činnost. V tabulce i na obrázku jsou kritické cesty znázorněny červenou barvou. Podle předchozích výpočtů se kritická cesta v grafu nachází mezi uzly:

0-1-5-7-11-10-12



Obrázek 5.7: Kritická cesta v grafu PERT

Tyto kritické činnosti musí být pod přísným dohledem managementu, protože jakékoliv prodloužení doby projektu mezi těmito uzly vede k prodloužení celého projektu, proto jim

Činnost	**I**	**J**	$\mathbf{t_c}$	**MZ**	**MK**	**PK**	**PZ**	**ČR**	$\mathbf{D^2_{t_c}}$
A	0	1	2,00	0,00	2,00	2,00	0,00	**0**	0,1111
B	0	2	5,00	0,00	5,00	6,00	1,00	1,00	0,1111
C	0	3	2,50	0,00	2,50	8,00	5,50	5,50	0,0278
D	1	5	7,00	2,00	9,00	9,00	2,00	**0**	0,1111
E	1	2	0,50	2,00	2,50	6,00	5,50	3,50	0,0069
F	2	5	3,00	5,00	8,00	9,00	6,00	1,00	0,1111
G	2	3	0,50	5,00	5,50	8,00	7,50	2,50	0,0069
H	3	4	0,00	5,50	5,50	0,00	0,00	-5,50	0,0000
I	3	5	1,00	5,50	6,50	9,00	8,00	2,50	0,0278
J	3	6	4,50	5,50	10,00	12,50	8,00	2,50	0,0278
K	4	0	0,00	5,50	5,50	0,00	0,00	-5,50	0,0000
L	5	7	1,50	9,00	10,50	10,50	9,00	**0**	0,0278
M	6	8	1,00	11,50	12,50	13,50	12,50	1,00	0,0278
N	6	9	3,00	11,50	14,50	19,00	16,00	4,50	0,1111
O	7	6	1,00	10,50	11,50	12,50	11,50	1,00	0,0278
P	7	8	2,50	10,50	13,00	13,50	11,00	0,50	0,1111
Q	7	11	7,00	10,50	17,50	17,50	10,50	**0**	0,1111
R	8	9	5,50	13,00	18,50	19,00	13,50	0,50	0,2500
S	9	10	1,00	18,50	19,50	20,00	19,00	0,50	0,0278
U	11	10	2,50	17,50	20,00	20,00	17,50	**0**	0,0278
V	10	12	9,00	20,00	29,00	29,00	20,00	**0**	0,1111

Tabulka 5.3: Metoda určení kritické cesty v grafu

musí být věnována maximální pozornost. Celková doba trvání projektu je **29 pracovních dní**. Celý projekt bude tedy trvat necelý pracovní měsíc. Pro upřesnění, převedení výsledku na kalendářní dny bude délka ukončení trvání projektu 39 dní. Pracovní týden má 5 dní, o víkendu se v posuzovaném podniku nepracuje, proto se musí víkendové dny zahrnout do délky trvání projektu, pokud má být délka trvání projektu posouzena z reálného hlediska. Z tabulky 5.3 jsou odečteny hodnoty pro realizaci celého projektu:

$$\begin{aligned} D^2_{t_c} &= 0{,}76 \\ D_{t_c} &= 0{,}87 \\ T_e &= 29 \text{ dní} \end{aligned}$$

Při určování pravděpodobnosti dodržení plánovaných termínů je doporučeno zvolit takový plánovaný termín ukončení celého projektu, který se co nejvíce blíží očekávanému, aby mohla být pravděpodobnost dodržení plánovaných termínů přesná a bylo možné určit normovanou náhodnou veličinu distribuční funkce, které jsou dostupné v tabulce A.9 a A.10.

Výpočet pravděpodobnosti dodržení plánovaného termínu lze provést pomocí vzorců 3.6 a 3.7 a pro plánovaný termín ukončení celého projektu za 28 pracovních dní, pravděpodobnost je:

$P(T \leq 28) = F\left(\frac{28-29}{0,87}\right) \Rightarrow F(u) = F(-1,15) \Rightarrow F(u) = 0,13$

Pravděpodobnost dodržení plánovaného termínu projektu pro plánovaný termín ukončení celého projektu za 30 pracovních dní:

$P(T \leq 30) = F\left(\frac{30-29}{0,87}\right) \Rightarrow F(u) = F(1,15) \Rightarrow F(u) = 0,87$

Pravděpodobnost dodržení plánovaného termínu během 28 pracovních dní je 13 % a během 30 pracovních dní je to 87 %. V případě rovnosti plánovaného termínu ukončení celého projektu a očekávaného termínu realizace celého projektu při celkem 29 pracovních dnech je pravděpodobnost dodržení plánovaného termínu 50 %, což je pro posuzovaný podnik přijatelné.

5.4 Ekonomické zhodnocení projektu

Nejdříve budou vyčísleny náklady spojené s aktivy podniku, pak tyto hodnoty budou spojeny s riziky, kterým je podnik vystaven, aby mohly být vyčísleny přínosy projektu a porovnána tak vhodnost realizace tohoto projektu. Poslední bod této kapitoly bude věnován výpočtům, zda-li je projekt z ekonomického hlediska výhodný.

5.4.1 Vyčíslení nákladů

Na začátku budou náklady rozděleny do třech skupin, a to investiční náklady, vyčíslitelné a nevyčíslitelné náklady. Konečné náklady budou uvedeny v USD. Kurz převodu Kč na USD je 0,051137836. Převod EUR na USD je 1,311173826. (35)

5.4.1.1 Investiční náklady

Investiční náklady jsou všechny náklady, které musí podnik pro úspěch projektu vynaložit a vychází ze všech doporučení.

- **OS licence** - podnik vlastní 50 počítačů a 5 notebooků. Z těchto 55 zařízení je na 38 zařízeních Windows XP Professional, na ostatních 17 zařízeních je Windows 7 Ultimate. Jelikož Microsoft ukončuje podporu ke dni 8.dubna 2014 (36), doporučuje se dokoupit Windows 7 upgrade licence v počtu 17 licencí, cena za jednu licenci je 219,99 USD ($). (37)

  $CN_{OS} = 17 * \$219,99 = \$3739,83$

- **SQL server** - aby mohl fungovat software od společnosti Safetica Technologies, musí být pořízen hardware a software pro SQL řešení Safetica software. W-Server s kalkulací pro 55 činí $9000.

- **Safetica** - licence včetně konzultací a práce vychází na 150 EUR nebo $200 na jeden počítač. (6)

  $CN_{Safetica} = 55 * \$200 = \$11000$

- **Záloha dat** - v případě záloh dat každého zaměstnance je doporučeno pořídit do serverovny datové úložiště (NAS server). Doporučený je WD Sentinel DX 4000 8TB v hodnotě 30860 Kč nebo $1578.

- **CIO** - nábor IT manažera bude v režii HR oddělení ve spolupráci ředitele podniku a managementu. Proto náklady spojené s náborem nebudou v tomto případě uvažovány. Plat IT manažera je stanoven na 45000 Kč, $2300 měsíčně. Zaměstnavatel musí odvést z platu zaměstnance zdravotní a sociální pojištění. Zdravotní pojištění činí z platu 45000 Kč celkem 4050 Kč, sociální pojištění 11250 Kč.

  $CN_{CIO} = 45000 + 4050 + 11250 = 60300\ Kč$

  $CN_{CIO} = 0,051137836 * 60300 = \$3084$

Položka	Náklad
OS Licence	3740
SQL Server	9000
Safetica	11000
CIO	3084
$\sum IN$	26824

Tabulka 5.4: Přehled investičních nákladů na projekt v USD

5.4.1.2 Vyčíslitelné náklady

Tyto odhadnuté náklady vycházejí z kapitoly 4.5.1, tedy z aktiv, které už podnik fyzicky vlastní a mohou být ohrožena riziky s nimi spojenými.

- **PC a NB** - náklady spojené s pořízením počítačů a notebooků. Náklady na jeden počítač v podniku jsou 18990 Kč a na notebook 22990 Kč.

  $CN_{HW} = (50 * 18990) + (5 * 22990) = 1064450\ Kč$

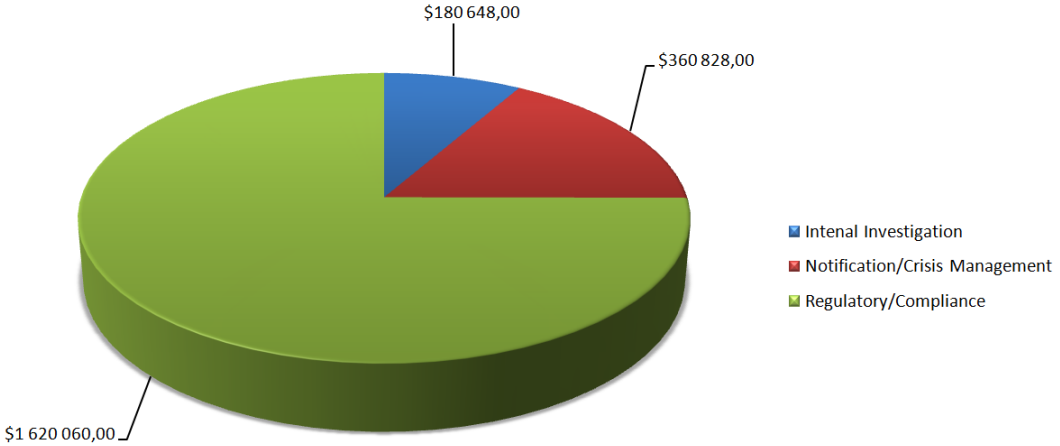
  $CN_{HW} = 0,051137836 * 1064450 = \$54434$

- **Periferie** - skupina periferie je vzhledem ke všem komponentům rozsáhlejší. Každý počítač musí mít dva monitory, notebook jeden monitor. Cena jednoho monitoru v podniku je 2990 Kč. Každý počítač a notebook má klávesnici a myš v hodnotě 230 Kč a 120 Kč. Tiskáren je v podniku celkem 10 kusů, z toho 8 kusů černobílé laserové tiskárny značky Kyocera (42500 Kč/ks) a 2 kusy multifunkční barevné laserové tiskárny značky OKI (63900 Kč/ks). Toner do Kyocery stojí 3734 Kč a výrobce udává tisk 15000 stran. Tonery do OKI stojí 10590 Kč (1332+3086+3086+3086) a výrobce udává tisk až 7300 stránek. Papíry na tisk se nakupují po 100 ks balení, kde balení obsahuje 500 listů papíru, cena jednoho balení je 80 Kč. Z dalších periferií, které podnik využívá ke své činnosti je automatický řezací stroj na dopisy (až 400 dopisů za minutu) v ceně 25 000 Kč a obálkovací stroj v hodnotě 160000 Kč. Pevné telefony v ceně 1150 Kč/ks má každý pracovník v podniku. K malé, poslední skupině periferií patří webkamery (5 ks v ceně 399 Kč/ks), headsety (10 ks v ceně 1200 Kč/ks).

  $CN_P = (105*2990)+(55*230)+(55*120)+(2*63990)+(8*42500)+(8*3734)+(2*10590)+(2*147000)+(100*80)+25000+160000+(5*399)+(10*1200)+(55*1150) = 313950 + 12650 + 6600 + 127980 + 340000 + 29872 + 21180 + 8000 + 185000 + 1995 + 12000 + 63250 = 1416477\ Kč$

  $CN_P = 0,051137836 * 1122477 = \$72436$

- **Data** - odhad ceny dat je založen na základě kalkulátoru nákladů odcizených dat z obrázku A.4. Předpoklad tohoto odhadu je kalkulace s počtem 13000 záznamů, složených z dat ohledně dodavatelů, odběratelů a interních záznamů zaměstnanců. Náklady by tedy vyšly odhadem \$166 na jeden záznam, celkem tedy \$2161536.



Obrázek 5.8: Struktura nákladů ztráty dat

- **Software** - software je ve složení Windows XP Professional (1900 Kč/1 licenci), Windows 7 Ultimate (5860 Kč/1 licenci), IBM Lotus Notes (182 EUR/1 licenci), Symantec Endpoint Protection (celková cena 81505 Kč), Microsoft Office 2007 Professional (7800 Kč/2 licence).

  $N_{SW} = (38 * 1900) + (17 * 5860) + 81505 + (55 * 7800/2) = 467825\ Kč$

  $N_{SW} = 55 * 182\ EUR = 10010\ EUR$

  $N_{SW} = (0,051137836 * 467825) + (1,311173826 * 10010) = \$37049$

- **Server** - jeden z nejdražších hmotných majetků v podniku. Společnost vložila do vybudování provozuschopnosti serverovny 550000 Kč, což odpovídá $28126.

- **Mobilní telefony** - tyto přístroje vlastní pouze vedoucí pracovníci a ředitel, čtyři mobilní telefony značky Nokia v hodnotě 2300 Kč/ks za kus a dva značky Blackberry v hodnotě 6600 Kč/ks.

  $CN_{MT} = (4 * 2300) + (2 * 6600) = 22400$ Kč

  $CN_{MT} = (0,051137836 * 22400) = \$1145$

- **Cenné papíry** - jsou stravenky a flexipassy. Stravenky v hodnotě 80 Kč dostává každý zaměstnanec za odpracovaný den (ale fyzicky je dostává až za odpracovaný měsíc), měsíc má 20 pracovních dní. Flexipassy v hodnotě 500 Kč za odpracovaný měsíc na jednoho zaměstnance. Cenné papíry jsou uschovány v trezoru, kam mají přístup pouze dvě osoby, případná pravděpodobnost ztráty je tedy minimální, přesto se musí s těmito náklady kalkulovat.

  $CN_{CP} = (55 * 20 * 80) + (55 * 500) = 115500$ Kč

  $CN_{CP} = (0,051137836 * 115500) = \$5906$

- **Kancelářské potřeby** - tužky, podložky pod myš, kalkulačky, šanony, pořadače, korektory apod. v ceně 88715 Kč.

  $CN_{KP} = 88715$ Kč

  $CN_{KP} = (0,051137836 * 88715) = \$4537$

- **Kancelářský nábytek** - židle, stoly, skříně v hodnotě 120000 Kč.

  $CN_{KN} = 120000$ Kč

  $CN_{KN} = (0,051137836 * 120000) = \$6137$

Položka	**Náklad**
PC & NB	54434
Periferie	72436
Data	2161536
Software	37049
Server	28126
Mobilní telefony	1145
Cenné papíry	5906
Kancelářské potřeby	4537
Kancelářský nábytek	6137
Kuchyňské vybavení	1023
$\sum VYN$	2344203

Tabulka 5.5: Přehled vyčíslitelných nákladů v USD

- **Kuchyňské vybavení** - varné konvice, mikrovlnné trouby, nádobí, příbory, sklenice, kávovar atd. v hodnotě 20000 Kč.

  $CN_{KV} = 20000$ Kč

  $CN_{KV} = (0,051137836 * 20000) = \$1023$

5.4.1.3 Nevyčíslitelné náklady

Mezi nevyčíslitelné náklady patří tištěné a elektronické faktury, ostatní dokumentace, bezpečnostní zařízení, IS SAP, služby, know how, goodwill, image podniku, energie, vodné/stočné, infrastruktura, podnikové prostředí.

5.4.2 Přínosy a očekávaná peněžní hodnota

U přínosů bude vycházeno z nákladů, respektive přínosu podniku z důvodu zabránění vzniku tohoto nákladu. V praxi není jednoduché přesně určit, kdy jaký stav nastane, do jaké výše z celkových nákladů se mohou vyšplhat. S příjmy bude kalkulováno v plné výši oproti nákladům v případě vzniku bezpečnostního incidentu, který by mohl nějakým způsobem poškodit aktiva podniku.

Položka	**Náklad**
Tištěné faktury	-
Elektronické faktury	-
Ostatní dokumentace	-
Bezpečnostní zařízení	-
IS SAP	-
Služby	-
Know how	-
Goodwill	-
Image podniku	-
Energie	-
Stočné	-
Infrastruktura	-
Podnikové prostředí	-
$\sum NEN$	-

Tabulka 5.6: Seznam nevyčíslitelných nákladů

5.4.2.1 Přínosy

V následující tabulce je uveden přehled přínosů. Jedná se o úsporu nákladů v případě zabránění vzniku bezpečnostního incidentu. Výpočet je proveden na základě propojení údajů z matice rizik, uvedené v kapitole 4.5.4 tabulce 4.8 a vypočtených nákladů v kapitole 5.4, doplněné o další aktiva s tímto rizikem spojené. Pokud je ve výpočtu uvedena nula, znamená to, že jsou zde zahrnuty i nevyčíslitelné náklady. Přínosy u jednotlivých položek jsou rovny jejím celkovým vypočteným nákladům.

Selhání hardware	= 54434+72436+28126	=	$154996
Selhání software	= 37049+0	=	$37049
Zastaralost hardware	= 54434+72436+28126	=	$154996
Krádež aktiva	= 5878+2161536+0+1145+5906+4537+6137+		
	+1023	=	$2186162
Zlomyslné kódy	= 0+37049	=	$37049
Výpadky sítě	= 28126+0	=	$28126
Vzniklý požár	= 54434+28126+0+72436+1145+5906+4537+		
	+6137+1023	=	$173744
Vnější útoky	= 28126+2161536+1145	=	$2190807
Zpronevěření aktiv	= 0+0+0	=	$0
Neúmyslná modifikace	= 0+2161536+0	=	$2161536
Selhání komunikace	= 0	=	$0
Hrozba epidemie	= 0	=	$0

Některé výpočty jsou doplněny i o aktiva, která v matici rizik není uvedena. Veškeré

přínosy podniku jsou shrnuty v tabulce 5.7. V konečném součtu všech přínosů je částka $7124465, zároveň je to i hodnota nákladů v případě, kdyby nastaly všechny bezpečnostní incidenty v plném rozsahu ve vztahu ke všem aktivům v jeden jediný okamžik. Taková pravděpodobnost vzniku nenadálé situace je minimální. Z hlediska ekonomického přínosu je toto vyčíslení vhodné, pokud má být posouzena výhodnost realizace projektu, respektive porovnání investičních nákladů s přínosy.

Investiční náklady na realizaci projektu jsou dohromady $26824. Pokud by se projekt bezpečnostní politiky realizoval, zabránilo by se vzniku bezpečnostních incidentů, přínosy by tedy byly v celkové hodnotě $7124465, v porovnání s náklady na investici jednoznačně tuto částku přínosy převyšují. Existuje samozřejmě pravděpodobnost, pokud nějaký bezpečnostní incident nastane, že ztráta nebude v plné výši. Realizace projektu se tedy z ekonomického hlediska doporučuje.

Incident	**Přínos**
Selhání hardware	154996
Selhání software	37049
Zastaralost hardware	154996
Krádež aktiva	2186162
Zlomyslné kódy	37049
Výpadky sítě	28126
Vzniklý požár	173744
Vnější útoky	2190807
Neúmyslná modifikace	2161536
$\sum Incidenty$	7124465

Tabulka 5.7: Přínosy v USD

5.4.2.2 Očekávaná peněžní hodnota

V této podkapitole budou porovnány očekávané peněžní hodnoty rozdílem mezi náklady a přínosy z určené pravděpodobnosti vzniku nákladů nebo přínosů. Tato pravděpodobnost je odvozena z tabulky 4.8. Po realizaci projektu je expertním odhadem je stanovena výše nákladů v případě vzniku bezpečnostního incidentu, které budou porovnány s přínosy za určené pravděpodobnosti vzniku nákladů (PN).

Pravděpodobnost vzniku nákladů na procenta vychází z údajů nabývajících maximálně hodnotu 5, tedy 100 % / 5 = 20 % na jeden bod. Těchto 20 % roznásobíme mezi pravděpodobnosti vzniku nákladů, analogicky se provede s pravděpodobností přínosů.

Rozdílem přínosů a nákladů projektu nám vznikne očekávaná peněžní hodnota (OPH). Pokud bude dosáhneme kladného čísla, je investice vhodná a čím vyšší tato hodnota je, tím lepší byla investice do projektu v této oblasti.

Z tabulky 5.8 je patrné, že investice do projektu bezpečnostní politiky je doporučena.

Incident	Přínos	Náklad	PN	OPH
Selhání hardware	154996	61858	3,50	3199
Selhání software	37049	23584	2,00	12796
Zastaralost hardware	154996	66927	3,34	6751
Krádež aktiva	2186162	85465	3,67	518788
Zlomyslné kódy	37049	16915	2,50	10067
Výpadky sítě	28126	20150	3,00	-840
Vzniklý požár	173744	172404	2,25	17977
Vnější útoky	2190807	123873	2,50	1033467
Neúmyslná modifikace	2161536	125840	2,00	1246586

Tabulka 5.8: Očekávaná peněžní hodnota v USD

5.4.3 Zhodnocení investice

Na základě čisté současné hodnoty (NPV) bude posouzena výhodnost investice do projektu a její dobu návratnosti.

Veškeré hodnoty potřebné pro výpočet těchto ukazatelů byly získány z údajů podniku uvedené v kapitole A.6. Investiční projekt s životností 5 let spočívá v investici $23740 v první fáze investice. V následujících letech provozu jsou investiční náklady zvýšené vždy o roční mzdové náklady $37008. Předpokládá se WACC 11,3 % p.a. Příjmy během provozu projektu fyzicky vznikat nebudou, proto s nimi nebude kalkulováno. Z předchozích informací bude vypočítán ukazatel ČSH.

Rok	0.	1.	2.	3.	4.	5.
IN	23,740	37,008	37,008	37,008	37,008	37,008
CF	-23,740	195293,548	218963,622	232942,239	253381,827	269514,102
WACC	-	0,113	0,113	0,113	0,113	0,113
NPV	-	175465,901	176759,042	168951,772	165118,147	157799,518

Tabulka 5.9: Čistá současná hodnota v tis. USD

Součtem všech čistých současných hodnot v jednotlivých letech po odečtení investičních nákladů dostaneme výslednou hodnotu čisté současné hodnoty, podle které zjistíme, jestli je investiční projekt pro podnik přijatelný.

$\boldsymbol{NPV} = (175465,901+176759,042+168951,772+165118,147+157799,518)-23,740 = 844094,380 - 23,740 =$ **844070,640** (v tis. USD)

Čistá současná hodnota projektu je $844070640. Pokud má být zjištěna doba návratnosti investice, tak je patrné, že vzhledem k investičním nákladům bude doba návratnosti do jednoho roku. Přesná doba návratnosti investice se zjistí pomocí dalšího ukazatele.

Z výše uvedených ukazatelů je investiční projekt přijatelný. K výpočtu ekonomických ukazatelů byly použity interní údaje celého podniku, nikoliv pouze údaje podniku umístě-

$$
\begin{array}{lll}
\mathrm{TN}_p & = \frac{(23{,}740+37{,}008)}{195293{,}548} & = 0{,}0003111 \quad \text{(v letech)} \\
\mathrm{TN}_p & = 0,0003111 * 365 & = 0{,}11353688 \quad \text{(ve dnech)} \\
\mathrm{TN}_p & = 0,11353688 * 24 & = 2{,}724885111 \quad \text{(v hodinách)} \\
\mathrm{TN}_p & = 2,724885111 * 60 & = 163 \quad \text{(v minutách)}
\end{array}
$$

ného v České republice. Tyto údaje byly použity pro orientaci výhodnosti investičního projektu, které jsou ovlivněny úspěšností podniku jako celku. Důvodem výpočtu je i fakt, že sponzorem změny v podniku je ředitel podniku, sponzorem ředitele podniku je globální ředitel pro evropské pobočky, ředitel pro evropské podniky spadá pod kompetence jiného ředitele, větev schvalování a řízení se pak dostává k CEO v USA, proto je způsob využití dat a výpočtu ukazatelů vhodný.

Celkový závěr ekonomického zhodnocení investice je patrný z předchozích podkapitol realizace investičního projektu, kdy lze jednoznačně tuto investici doporučit. Na základě vypočítaných ukazatelů čisté současné hodnoty a doby návratnosti investice je zřejmé, jak jsou náklady investičního projektu skoro zanedbatelné v porovnání s celkovým hospodařením podniku (včetně volných prostředků na realizaci projektů). Čistá současná hodnota je kladná a doba návratnosti je 163 minut, projekt se doporučuje realizovat. Zde lze konstatovat, že záleží přímo na vedoucích pracovnících, kteří jsou zodpovědní za schvalování projektů na evropské úrovni, zda projekt schválí. V případě implementace projektu na všechny pobočky podniku by asi ukazatele nabývaly jiných hodnot, ale výpočet by pak byl mnohem složitější jak z hlediska obtížnosti, tak i délky trvání.

6 Závěr

Tématem této diplomové práce bylo posouzení informačního systému firmy a návrh změn. K posouzení byla vybrána finanční pobočka podniku, která je umístěna v Brně v ČR a pracuje v ní kolem 50 zaměstnanců. Cílem práce bylo posouzení informačního sytému SAP, který uvedený podnik používá a pomocí vybraných analýz odhalit kritický nedostatek tohoto informačního systému, nalézt řešení k jeho odstranění či optimalizaci spolu s ekonomickým zhodnocením aplikace doporučené implementace.

Podniková strategie je efektivní zpracovávání faktur a realizace finančního toku bez účasti faktoringové společnosti, centralizace služeb přesunutím ostatních týmů podobného zaměření do ČR. Analýzou byla posouzena a vyhodnocena řada faktorů, které mohou posunout pozitivně podnik v dalším rozvoji a úspěchu v podnikání. Z analýzy také vyplynulo, že zásadním kritickým nedostatkem celého systému je chybějící bezpečnostní politika, která může způsobit podniku kromě potíží i další finanční a prestižní ztráty.

PEST analýza posoudila vnější faktory, které podnik ovlivňují, např. legislativa, nezaměstnanost, dotace, inflace, mzdové náklady, ceny energií, clo, DPH apod. K faktorům, které lze ovlivnit, patří např. zaměstnanost, kdy podnik díky dotacím na zvýšení zaměstnanosti a vzdělanosti může na jedné straně finance ušetřit, na druhé straně zvýšit kvalitu vzdělanosti a tím posunout v pozitivním slova smyslu podnik na vyšší úroveň.

SWOT metoda kombinuje analýzu vnitřního a vnějšího prostředí podniku, na základě které bylo zjištěno, že podnik má výhodu v počtu vzdělaných a zkušených zaměstnanců díky nadstandardním platům a benefitům. Naopak tato analýza poukazuje opět na nedostatečnou bezpečnostní politiku.

Metoda rozboru 7S faktorů se zaměřuje na popis vnitřního prostředí podniku. Součástí této analýzy je organizační struktura, zde nebyly shledány problémy.

V další části práce byla posuzována efektivnost informačního systému a jeho osmi klíčových oblastí. Metoda je založena na vyplnění elektronických dotazníků respondenty pracujícími v daném podniku s tím rozdílem, že při posouzení efektivnosti informačního systému dotazníky vyplňují všichni zaměstnanci, při posouzení osmi klíčových oblastí IS dotazníky vyplňují pouze vedoucí pracovníci. Dále jsou dotazníky vyhodnoceny v referenční databázi ZEFIS s daty podniků podobné velikosti a oboru podnikání. Na základě výsledků obou metod vyplynulo, že uživatelé informační systém využívají ke své pracovní činnosti většinu pracovního dne a nevyhovuje jim složitost ovládání informačního systému. V této oblasti je doporučen trénink a dlouhodobá praxe s IS SAP. Naopak přesnost a úplnost dat poskytovaných systémem je na velmi dobré úrovni.

Zásadním výsledkem analýzy, jak již bylo uvedeno, je kritický nedostatek bezpečnostní politiky. Z analýzy vyplynulo k tomuto nedostatku, že zde chybí IT manažer, zodpovědný za implementaci dodržování a kontrolu bezpečnostní politiky. S tím souvisí i neexistující vnitropodnikové dokumenty ohledně informačních systémů a bezpečnostní politiky, i když sice základní pravidla existují, ale nejsou nikým vyžadována ani kontrolována a existují pouze na elementární úrovni.

Ze zjištění pomocí Lewinova modelu, který využil poznatků z rozboru 7S faktorů, je doporučeno určit ředitele podniku v České republice jako sponzora změny a vedoucí pracovníky jako agenty změn v oblasti bezpečnostní politiky.

K analýze možnosti vytvoření bezpečnostní politiky dle standardu ISO/IEC 27005 bylo nutno provést identifikaci aktiv. Ohodnocení aktiv je založeno na důležitosti, integritě a finanční ztrátě z hlediska informačního systému. Nejvyšší hodnoty 4,04 ze skupiny aktiv dosahuje nehmotný majetek.

Analýza hrozeb vychází z identifikace vybraných aktiv. Zde je posouzena pravděpodobnost vzniku hrozby a případná zranitelnost aktiva v případě vzniku bezpečnostního incidentu. Na základě provedených analýz bezpečnostní politiky je sestavena matice rizik, z které vyšlo najevo, že mezi nepřijatelná rizika patří krádež dat, selhání hardware a firemní komunikace.

V první řadě je tedy podniku doporučen nábor IT manažera (CIO), který bude za fungování a dodržování bezpečnostní politiky zodpovědný, nápomocni mu budou vedoucí pracovníci v podniku.

Selhání hardware je možné zabránit výběrem kvalitního dodavatele zboží a servisu v optimálním poměru kvalita/cena. Je vhodné sestavit seznam ověřených dodavatelů a servisů, který by IT manažer neustále aktualizoval.

Selhání firemní komunikace lze zabránit kvalitním složením managementu, který bude dobře motivovat své podřízené zaměstnance, vedoucí k profesionálnímu jednání s dodavateli a odběrateli, bude zlepšovat i interní komunikaci. Selhání komunikace se řadí k obtížněji ovlivnitelným faktorům v podniku.

Zabránění úniku dat je doporučeno pomocí Safetica software, který disponuje prevencí úniku dat na dálku pomocí Safetica Management Console, součástí je i správa zařízení, šifrování dat, blokování aktivity (reporty uživatelské aktivity) a měření produktivity zaměstnanců. Stochastickou metodou PERT bylo zjištěno, že implementace bezpečnostní politiky předpokládá práci v délce 29 pracovních dní.

Při porovnání úspory nákladů v hodnotě $7124465 s investičními náklady $26824 a očekávanou peněžní hodnotou $2848791, se implementace bezpečnostní politiky doporučuje. Čistá současná hodnota je $844070410 a doba návratnosti investic je 163 minut. Oba ukazatele jsou ovlivněny použitými údaji mateřského podniku a ne pouze jeho pobočky v České republice.

Závěrem lze tedy konstatovat, že lze jednoznačně implementaci bezpečnostní politiky v podniku doporučit. Pokud se podnik bude řídit doporučeními uvedenými v této práci, implementace bezpečnostní politiky bude úspěšná a lze ji pak implementovat i v ostatních pobočkách. Podnik tak bude více chráněn proti rizikům, která by mu mohla způsobit velké ztráty na všech úrovních.

7 Seznam použité literatury

(1) BASL, Josef a Roman BLAŽÍČEK. *Podnikové informační systémy: Podnik v informační společnosti*. 3., aktualiz. a dopl. vyd. Praha: Grada, 2012, 323 s. ISBN 978-80-247-4307-3.

(2) MOLNÁR, Zdeněk. *Efektivnost informačních systémů*. 2. rozš. vyd. Praha: Grada, 2001, 179 s. ISBN 80-247-0087-5.

(3) ŘEPA, Václav. *Podnikové procesy: Procesní řízení a modelování*. 2., aktualiz. a rozš. vyd. Praha: Grada, 2007, 281 s. ISBN 978-80-247-2252-8.

(4) SODOMKA, Petr a Hana KLČOVÁ. *Informační systémy v podnikové praxi*. 2., aktualiz. a rozš. vyd. Brno: Computer Press, 2010, 501 s. ISBN 978-80-251-2878-7.

(5) SAP Česká republika. *Ness zavedl komplexní informační systém pro ČEPS* [Online]. ©2008. [Cit. 2012-10-09]. Dostupné z: http://www.sap.com/cz/press.epx?pressid=10246.

(6) HALÍČEK, Josef. *Konzultace*. Safetica Technologies s.r.o., U Vodárny 2965/2, 616 00 Brno. 2.5.2013

(7) KOTLER, Philip. *Moderní marketing: 4. evropské vydání*. 1. vyd. Praha: Grada, 2007, 1041 s. ISBN 978-80-247-1545-2.

(8) JAKUBÍKOVÁ, Dagmar. *Strategický marketing*. 1. vyd. Praha: Grada, 2008, 269 s. ISBN 978-80-247-2690-8.

(9) BLAŽKOVÁ, Martina. *Marketingové řízení a plánování pro malé a střední firmy*. 1. vyd. Praha: Grada, 2007, 278 s. ISBN 978-80-247-1535-3.

(10) KOCH, Miloš. *ZEFIS*. Výzkumný portál Ústavu informatiky pro firmy. [Online] VUT, ©2010. [Cit. 2012-11-10]. Dostupné z: http://www.zefis.cz/index.php?id=341.

(11) HOLOUBEK, Josef. *Ekonomicko-matematické metody*. 2., nezměn. vyd. V Brně: Mendelova univerzita, 2010, 153 s. ISBN 978-80-7375-411-2.

(12) SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve podnicích a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010, 354 s. ISBN 978-80-247-3051-6.

(13) Khandelwal, B.C.P.K.K. *Project Planning and Control with PERT & CPM*. Firewall Media, 2002, 260 s. ISBN 978-81-318-0698-2.

(14) RAIS, Karel a Radek DOSKOČIL. *Operační a systémová analýza I: studijní text pro kombinovanou formu studia*. Vyd. 1. Brno: Akademické nakladatelství CERM, 2006, 2 sv. (59 s., s. 60-107). ISBN 80-214-3280-2.

(15) VÍTEČKOVÁ Miluše, PŘIDAL Petr a KOUDELA Tomáš. *Metoda PERT*. Výukový modul, VŠB - Technická univerzita Ostrava. [Online] ©2006 [Cit. 2013-02-25] Dostupné z: http://books.fs.vsb.cz/SystAnal/texty/26.htm.

(16) PETERS, Thomas J a Robert H WATERMAN. *In search of excellence: lessons from America's best-run companies*. 1st Warner print. New York: Warner Books, 1984 360 s. ISBN 0-446-38281-7.

(17) GÁLA, Libor, Jan POUR a Prokop TOMAN. *Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi, technologie informačních systémů, řízení a rozvoj podnikové informatiky*. 1. vyd. Praha: Grada, 2006, 482 s. ISBN 80-247-1278-4.

(18) MLÝNEK, Jaroslav. *Zabezpečení obchodních informací*. Vyd. 1. Brno: Computer Press, c2007, vi, 154 s. ISBN 978-80-251-1511-4.

(19) STEINER, František. *Případová studie analýzy rizik informační bezpečnosti*. [Online] ©2007. [Cit. 2013-03-03]. ISBN 978-80-7043-535-9 Dostupné z: http://bpm-tema.blogspot.cz/2007/11/ppadov-studie-analzy-rizik-informan.html.

(20) Business of Security. *Fair - ISO/IEC 27005 Cookbook*. [Online] ©2010. [Cit. 2013-03-03]. ISBN 1-931624-87-9. Dostupné z: http://www.businessofsecurity.com/docs/FAIR%20-%20ISO_IEC_27005%20Cookbook.pdf.

(21) POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, 309 s. ISBN 80-86898-38-5.

(22) BANGEMANN, Tom Olavi. *Shared Services In Finance And Accounting*. Gower Publishing Ltd., 2005. 246 s. ISBN 978-0-566-08607-6.

(23) SCHWALBE, Kathy. *Řízení projektů v IT*. Brno: Computer Press, 2007. 720 s. ISBN 978-80-251-1526-8.

(24) GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. *Podniková informatika*. 2. přeprac. a aktualiz. vyd. Praha: Grada. 2009, 496 s. ISBN 978-80-247-2615-1.

(25) Portál veřejné zprávy. *Zákoník práce 262/2006 Sb.*. [Online] ©2013. [Cit.2013-03-07]. Dostupné z: http://portal.gov.cz/app/zakony/zakon.jsp?page=0&nr=262~F2006&rpp=15#seznam.

(26) Národní bezpečnostní úřad. *Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.* [Online] [Cit. 2013-03-07]. Dostupné z: http://www.nbu.cz/cs/pravni-predpisy/zakon-c-4122005.

(27) Demografie. *Populační vývoj ČR.* [Online] ©2004-2009. [Cit. 2013-03-03]. ISSN 1801-2914. Dostupné z: http://www.demografie.info/?cz_popvyvoj.

(28) Český Statistický Úřad. *Inflace, spotřebitelské ceny.* [Online] ©2013. [Cit. 2013-03-08]. Dostupné z: http://www.czso.cz/csu/redakce.nsf/i/inflace_spotrebitelske_ceny.

(29) Česká strana sociálně demokratická. *Vláda by měla urychleně řešit nezaměstnanost mladých lidí v ČR.* [Online] ©2013. [Cit. 2013-03-09]. Dostupné z: http://www.cssd.cz/media/tiskove-zpravy/vlada-by-mela-urychlene-resit-nezamestnanost-mladych-lidi-v-cr.

(30) Národní bezpečnostní úřad. *Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění vyhlášky č. 453/2011 Sb.* [Online]. [Cit. 2013-03-09]. Dostupné z: http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/vyhlaska-c-5232005.

(31) Výplata. *Příspěvek zaměstnavatelům, kteří vytvářejí nová pracovní místa.* Informace ze světa financí a peněz online. [Online] ©1998-2013. [Cit. 2013-03-10]. Dostupné z: http://www.vyplata.cz/zamestnavatel/prispevkystatuzamestnavateli.php.

(32) Anti-virus Software Review. *2013 Compare The Best Antivirus Software Products* [Online] ©2013. [Cit. 2013-04-19]. Dostupné z: http://anti-virus-software-review.toptenreviews.com.

(33) Safetica. *Měření produktivity* [Online]. ©1999-2013. [Cit. 2013-04-21]. Dostupné z: http://www.safetica.cz/reseni/mereni-produktivity.

(34) Safetica. *Sreenshoty* [Online]. ©1999-2013. [Cit. 2013-04-21]. Dostupné z: http://www.safetica.cz/produkt/screenshoty.

(35) Finance. *Kalkulátor převodu měn (podle kurzovního lístku ČNB)* [Online] ©2013. [Cit. 2013-05-03]. Dostupné z: http://www.finance.cz/makrodata-eu/kalkulacky-aplikace/prevodnik-men/index.phtml#prevodcnb.

(36) Windows. *Končí podpora systému Windows XP* [Online] ©2013. [Cit. 2013-05-04]. Dostupné z: http://windows.microsoft.com/cs-cz/windows/end-support-help.

(37) Microsoft Store. *Windows 7 Ultimate* [Online] ©2013. [Cit. 2013-05-04]. Dostupné z: http://www.microsoftstore.com/store/msusa/en$_US$/*pdp*/*productID*.253678200.

(38) Tech//404. *Tech//404 Data Loss Cost Calculator* [Online] ©2006-2010. [Cit. 2013-05-05]. Dostupné z: http://www.tech-404.com/calculator.html.

(39) FOTR, Jiří a Ivan SOUČEK. *Podnikatelský záměr a investiční rozhodování*. 1. vyd. Praha: Grada, 2005, 356 s. ISBN 80-247-0939-2.

Seznam tabulek

Seznam obrázků

Seznam příloh

A Přílohy

A.1 Posouzení informačního systému pomocí Zefis

V první části jsou zpracované dotazníky ohledně efektivnosti informačního systému, následně pokračuje ohodnocení jednotlivých částí informačního systému HOS.

A.1.1 Efektivita informačního systému

Posuzovaný podnik

V tomto odstavci jsou uvedeny informace o posuzovaném podniku, jednak z dotazníku tamějšího analytika (toho, kdo provedl průzkum), jednak z odpovědí zaměstnanců. Pokud tyto hodnoty neodpovídají skutečnosti, další výsledky nejsou věrohodné. V takovém případě je potřeba zkontrolovat a opravit dotazník tamějšího analytika. Pokud jsou divné odpovědi pracovníků, pak pravděpodobně jejich informovanost o položené otázce není dostatečná.

Porovnáním výsledků v tomto odstavci se skutečností získáme představu o věrohodnosti posouzení ostatních částí.

Analytik	
Velikost posuzovaného podniku:	10-49 zaměstnanců
Oblast podnikání:	Finanční činnosti
Země:	Česká, Slovenská republika
Orientační počet počítačů	50-99

Naši pracovníci		
Velikost posuzovaného podniku:	50-99	(16 / 23)
Velikost posuzovaného podniku:	více než 1000	(3 / 23)
Oblast podnikání:	Finanční činnosti	(15 / 23)
Oblast podnikání:	Výrobní podnik	(5 / 23)
Země:	Česká, Slovenská republika	(16 / 23)
Země:	Ostatní země	(1 / 23)
Orientační počet počítačů	50-99	(17 / 23)
Orientační počet počítačů	100-199	(3 / 23)

Pro zpracování analýzy je nezbytné mít alespoň 3 dotazníky vyplněné zaměstnanci podniku, ale podařilo se vyplnit celkem 23 dotazníků. To znamená, že počet dotazníků je dostatečný k posouzení celého podniku, platnost výsledků lze zobecnit na celý podnik, byť s možnými, ale nepříliš pravděpodobnými nepřesnostmi.

Posuzovaný informační systém

Nyní se zaměříme na posuzovaný informační systém, který respondenti popisovali. V dotazníku byli požádáni, aby popisovali informační systém, se kterým nejvíce pracují (pro případ, že používají více systémů). Velmi zde záleží na nastavení parametrů vyhodnocení. Pokud posuzovaný analytik stanovil posouzení celého podniku, bez vybraných skupin pracovníků a časového období průzkumu, ve výsledcích mohou pracovníci hodnotit více systémů, což zkresluje vypovídací schopnost - výsledky se potom týkají firmy jako celek.

Lepší výsledky dostaneme, pokud zkoumáte jeden určitý systém se skupinou pracovníků, kteří jej používají. Toho lze docílit průzkumem v určitém časovém intervalu a výběrem pouze dotazníků z tohoto období k hodnocení.

Jaký informační systém převážně používáte? V této subkapitole se posuzuje, jak je informační systém který používáte velký. Velikost systémů by měla být v souladu s velikostí firmy.

Naši pracovníci		
Velký systém, ERP a podobně v ceně řádově stovky tisíc až miliony Kč.	(20 / 23)	86 %
Nevím	(2 / 23)	8 %
Používám jen kancelářský balík, např. Microsoft Office	(2 / 23)	4 %
Pracovníci ostatních firem		
Velký systém, ERP a podobně v ceně řádově stovky tisíc až miliony Kč.	(1896 / 4156)	45 %
Malý systém, v ceně řádově desítky tisíc Kč.	(1071 / 4156)	25 %
Používám jen kancelářský balík, např. Microsoft Office	(625 / 4156)	15 %

Odpovědi respondentů jsou odlišné od odpovědí srovnávaných firem, viz test dobré shody.

Jak je informační systém starý? Stáří informačního systému do jisté míry vypovídá o jeho kvalitách. U velkých systémů je přijatelné delší stáří, malé systémy se obvykle mění častěji.

Naši pracovníci		
Nevím	(16 / 23)	69 %
1 - 3 roky	(3 / 23)	13 %
3 - 5 let	(2 / 23)	8 %
Pracovníci ostatních firem		
1 - 3 roky	(955 / 4156)	22 %
5 - 10	(946 / 4156)	22 %
3 - 5 let	(846 / 4156)	20 %

Jaké řešení informačního systému máte? V této subkapitole se posuzuje, zda používáte informační systém typový, hotové a kustomizované řešení jako ERP systémy, nebo zda je informační systém vytvořený na míru podniku, případně pronajatý a provozovaný u některého poskytovatele.

Naši pracovníci		
Hotové řešení / koupený systém (Například SAP, Microsoft Dynamics atp.)	(21 / 23)	91 %
Nevím	(2 / 23)	8 %
Pracovníci ostatních firem		
Hotové řešení / koupený systém (Například SAP, Microsoft Dynamics atp.)	(2217 / 4159)	53 %
Vyvinutý na zakázku cizí firmou	(721 / 4159)	17 %
3 - 5 let	(664 / 4159)	15 %

Silné stránky posuzovaného systému Naopak zde uvedené věci jsou ty, které považují naši uživatelé za nejlepší na posuzovaném informačním systému a se kterými jsou nejvíce spokojeni.

Naši pracovníci		
přesnost a úplnost dat poskytovaných systémem	(14 / 22)	31 %
rychlost odezvy/ zpracování	(10 / 44)	22 %
programové vybavení	(5 / 44)	22 %

Pracovníci ostatních firem		
uživatelská přívětivost a snadnost ovládání	(1131 / 7075)	15 %
přesnost a úplnost dat poskytovaných systémem	(1114 / 7075)	15 %
programové vybavení	(971 / 7075)	13 %

Slabé stránky posuzovaného systému Zde jsou uvedeny tři věci, seřazené podle četnosti, které našim uživatelům nejvíce vadí na posuzovaném informačním systému.

Naši pracovníci		
uživatelská přívětivost a snadnost ovládání	(10 / 24)	41 %
rychlost odezvy/ zpracování	(5 / 24)	20 %
přesnost a úplnost dat poskytovaných systémem	(3 / 24)	12 %

Pracovníci ostatních firem		
rychlost odezvy/ zpracování	(1555 / 5451)	28 %
uživatelská přívětivost a snadnost ovládání	(996 / 5451)	18 %
podpora	(899 / 5451)	16 %

Naši zaměstnanci

V této kapitole se podíváme na tamější pracovníky, kteří se zúčastnili průzkumu. Zjišťuje se jejich vzdělání, znalost práce s počítačem a výsledky se porovnávají s ostatními podniky.

Jaká je struktura pracovníků v průzkumu Tato informace sděluje, kteří pracovníci se průzkumu účastnili, rozčlenění podle svého profesního zařazení.

Naši pracovníci		
Výkonný pracovník v podpůrných procesech firmy	(17 / 22)	77 %
Výkonný pracovník v hlavních procesech firmy	(2 / 22)	9 %
Řídicí pracovník podpůrných procesů firmy	(2 / 22)	9 %

Pracovníci ostatních firem		
Výkonný pracovník v hlavních procesech firmy	(1380 / 4165)	33 %
Výkonný pracovník v podpůrných procesech firmy	(1370 / 4165)	32 %
Řídicí pracovník hlavních procesů firmy	(770 / 4165)	18 %

Jaké je nejčastější vzdělání pracovníků v průzkumu Tato informace nám ukazuje, jaké je nejčastější vzdělání pracovníků posuzovaného podniku a u pracovníků srovnatelných firem.

Naši pracovníci		
Ekonomika	(13 / 23)	56 %
Humanitní vědy	(6 / 23)	26 %
Obecné	(3 / 23)	13 %

Pracovníci ostatních firem		
Ekonomika	(1368 / 4168)	32 %
Technika	(1242 / 4168)	29 %
Informatika	(577 / 4168)	13 %

Jaké je nejvyšší vzdělání pracovníků v průzkumu Tato informace nám ukazuje, jaké je nejvyšší vzdělání pracovníků posuzovaného podniku a u pracovníků srovnatelných firem.

Naši pracovníci		
Vysokoškolské, MBA	(15 / 23)	65 %
Středoškolské	(6 / 23)	26 %
Základní	(2 / 23)	8 %
Pracovníci ostatních firem		
Vysokoškolské, MBA	(2343 / 4166)	56 %
Středoškolské	(1656 / 4166)	39 %
Vyšší než vysokoškolské, vědecká hodnost (Ph.D., atd)	(120 / 4166)	2 %

Jaký je věk pracovníků v průzkumu Zde vidíme věková pásma pracovníků posuzovaného podniku, kteří se zúčastnili průzkumu, a srovnatelných firem.

Naši pracovníci		
21 - 40	(23 / 23)	100 %
Pracovníci ostatních firem		
21 - 40	(2844 / 4169)	68 %
41 - 60	(1214 / 4169)	29 %
vice než 60	(71 / 4169)	1 %

Jak dlouho pracovníci pracují pro podnik Zde vidíme pásma délky zaměstnání u pracovníků posuzovaného podniku, kteří se zúčastnili průzkumu, a u pracovníků srovnatelných firem.

Naši pracovníci		
1 až 3 roky	(13 / 23)	56 %
3 měsíce až 1 rok	(8 / 23)	34 %
méně než 3 měsíce	(2 / 23)	8 %
Pracovníci ostatních firem		
Více než 3 roky	(2418 / 4166)	58 %
1 až 3 roky	(1084 / 4166)	26 %
3 měsíce až 1 rok	(518 / 4166)	12 %

Jaký mají vztah k počítačům Poměrně důležitá informace, ukazuje schopnost pracovníků posuzovaného podniku pracovat s informačními systémy.

Naši pracovníci		
Dobrý, umím s nimi dobře pracovat, využívám je ve většině případů, kdy to povaha práce/ zábavy umožňuje	(13 / 23)	56 %
Neutrální, umím s nimi pracovat na požadované úrovni, ale nemám o ně velký zájem	(9 / 23)	39 %
Vynikající, je to můj koníček / profese	(1 / 23)	4 %
Pracovníci ostatních firem		
Dobrý, umím s nimi dobře pracovat, využívám je ve většině případů, kdy to povaha práce/ zábavy umožňuje	(2214 / 4169)	53 %
Vynikající, je to můj koníček / profese	(1156 / 4169)	27 %
Neutrální, umím s nimi pracovat na požadované úrovni, ale nemám o ně velký zájem	(765 / 4169)	18 %

Jak často používají informační systém Poměrně důležitá informace, ukazuje jak často potřebují pracovníci posuzovaného podniku pracovat s informačními systémy.

Naši pracovníci		
Většinu pracovního dne	(23 / 23)	100 %
Pracovníci ostatních firem		
Většinu pracovního dne	(2664 / 4169)	63 %
Několikrát denně	(1027 / 4169)	24 %
Několikrát týdně	(421 / 4169)	10 %

Podpora dalšího vzdělávání pracovníků Zjišťuje se, jak posuzovaný podnik podporuje další vzdělávání pracovníků ve srovnání s ostatními podniky.

Naši pracovníci		
Spíše ano	(14 / 23)	60 %
Ano, aktivně. Podporuje další vzdělávání finančně nebo některými úlevami	(9 / 23)	39 %
Pracovníci ostatních firem		
Spíše ano	(358 / 873)	41 %
Spíše ne	(183 / 873)	20 %
Ano, aktivně. Podporuje další vzdělávání finančně nebo některými úlevami	(182 / 873)	20 %

Úroveň podpory

Tato kapitola posuzuje, jakou podporu v práci s informačním systémem mají naši pracovníci. Jde o důležitý faktor efektivního využívání informačních systémů. Při špatné úrovni podpory se snižuje efektivita užití. Výsledky jsou opět porovnány s úrovní podpory ve vybraných podnicích.

Spokojenost pracovníků s podporou informačních systémů Zde se srovnává, zda jsou naši pracovníci spokojeni s podporou informačních systémů obecně, ve srovnání s pracovníky ostatních firem. Je třeba vzít v úvahu, že technickou podporu (opravy počítačů, instalace software) může dělat obecně jiný subjekt než uživatelskou podporu (práce s informačním systém, potíže s daty). Tato spokojenost v sobě zahrnuje spokojenost jak s technickou, tak uživatelskou podporou.

Naši pracovníci		
Jsem spíše spokojen/a	(12 / 23)	52 %
Jsem velmi spokojen/a, podpora plně odpovídá potřebám	(7 / 23)	30 %
Podpora je průměrná	(3 / 23)	13 %
Pracovníci ostatních firem		
Jsem spíše spokojen/a	(358 / 873)	38 %
Podpora je průměrná	(1264 / 4143)	30 %
Ano, aktivně. Podporuje další vzdělávání finančně nebo některými úlevami	(577 / 4143)	13 %

Kdo zajišťuje technickou podporu Zde jsou uvedeny odpovědi zaměstnanců na otázku, kdo zajišťuje jejich technickou podporu, tedy instalace počítačů, opravy počítačů, výměna tonerů v tiskárnách a podobně.

Naši pracovníci		
Externí pracovník z jiné firmy	(17 / 23)	73 %
Interní pracovník posuzovaného podniku z útvaru informačních systémů	(4 / 23)	17 %
Mám podporu, ale nevím zde je to interní či externí pracovník	(2 / 23)	8 %
Pracovníci ostatních firem		
Interní pracovník posuzovaného podniku z útvaru informačních systémů	(1926 / 3258)	59 %
Podpora je průměrná	(903 / 3258)	27 %
Ano, aktivně. Podporuje další vzdělávání finančně nebo některými úlevami	(199 / 3258)	6 %

Kdo zajišťuje uživatelskou podporu Zde jsou uvedeny odpovědi zaměstnanců na otázku, kdo zajišťuje jejich uživatelskou podporu, tedy radu a pomoc v případě potíží s informačním systémem, daty a podobně.

Naši pracovníci		
Interní pracovník posuzovaného podniku z útvaru informačních systémů	(15 / 23)	65 %
Externí pracovník z jiné firmy	(6 / 23)	26 %
Mám podporu, ale nevím zde je to interní či externí pracovník	(1 / 23)	4 %
Pracovníci ostatních firem		
Interní pracovník posuzovaného podniku z útvaru informačních systémů	(2288 / 3825)	59 %
Externí pracovník z jiné firmy	(825 / 3825)	21 %
Někdo jiný, kdo není pracovníkem útvaru informačních systémů, například někdo z kolegů	(450 / 3825)	11 %

Doba opravy počítače / technické závady Zde jsou uvedeny odpovědi zaměstnanců na otázku, jak dlouho musí průměrně čekat při požadavku na opravu jejich počítače. Jde o dost důležitou informaci. V případě dlouhého čekání na opravu dochází u pracovníků, kteří potřebují počítač ke své práci, k snížení produktivity práce či znemožnění jejich práce. Je třeba ale zvážit, zda se jedná o pracovníky, kteří nemohou bez počítače vykonávat svoji práci, nebo o ty, kteří potřebují počítač několikrát denně.

Naši pracovníci		
Méně než hodinu	(12 / 23)	52 %
Méně než 1 den	(6 / 23)	26 %
Méně než 4 hodiny	(5 / 23)	21 %
Pracovníci ostatních firem		
Méně než 1 den	(912 / 3254)	28 %
1-2 dny	(826 / 3254)	25 %
Méně než 4 hodiny	(621 / 3254)	19 %

Doba instalace nebo změny programů Zde jsou uvedeny odpovědi zaměstnanců na otázku, jak dlouho musí průměrně čekat při požadavku na instalaci programů na jejich počítače nebo jejich aktualizaci. Tato doba není tak závažná jako řešení technických problémů s počítačem.

Naši pracovníci		
Méně než 4 hodiny	(9 / 23)	39 %
Méně než 1 den	(8 / 23)	34 %
Méně než hodinu	(4 / 23)	17 %

Pracovníci ostatních firem		
1-2 dny	(917 / 3251)	28 %
Méně než 1 den	(866 / 3251)	26 %
Méně než 4 hodiny	(441 / 3251)	13 %

Spokojenost pracovníků s uživatelskou podporou Zde se srovnává, zda jsou naši pracovníci spokojeni s uživatelskou podporou informačních systémů obecně, ve srovnání s pracovníky ostatních firem. Uživatelská podpora poskytuje radu a pomoc při práci s informačním systémem.

Naši pracovníci		
Jsem spíše spokojen/a	(11 / 23)	47 %
Jsem velmi spokojen/a, podpora plně odpovídá potřebám	(6 / 23)	26 %
Podpora je průměrná	(6 / 23)	26 %
Pracovníci ostatních firem		
Jsem spíše spokojen/a	(1048 / 2668)	39 %
Podpora je průměrná	(940 / 2668)	35 %
Jsem velmi spokojen/a, podpora plně odpovídá potřebám	(298 / 2668)	11 %

Úroveň řízení

Tato kapitola posuzuje některé oblasti, které se ukazují jako zdroj problémů v řízení podniku. Zkoumá, zda v podniku existuje manažer odpovědný za informační systémy (CIO - Chief Information Officer), do jaké míry jsou naši pracovníci seznámeni s podnikovou a informační strategií a zda ví, jak ovlivňují svojí prací výsledky firmy.

Je pochopitelné, že pracovníci firmy nemusí znát strategii detailně, ale měli by chápat hlavní cíle firmy, kam podnik směřuje, jaké má požadavky na své pracovníky (např. jejich chování k zákazníkům) a podobně.

Manažer informačních systémů Zkoumá se, zda je u posuzovaného podniku CIO, či nikoli. U malých firem CIO nebývá, někdy je funkce kumulovaná s jinou, ale i u malých firem by měl mít někdo na starost řízení informačních systémů.

Naši pracovníci		
Ano	(12 / 23)	52 %
Ne	(7 / 23)	30 %
Ano, ale pozice je kumulována s jinou	(4 / 23)	17 %

Pracovníci ostatních firem		
Ano	(726 / 1719)	42 %
Ne	(503 / 1719)	29 %
Ano, ale pozice je kumulována s jinou	(490 / 1719)	28 %

Znalost firemní strategie Orientační znalost firemní strategie ve smyslu chápání cílů firmy a jak má pracovník fungovat aby přispíval k dosažení těchto cílů je pokládána za důležitý kritický faktor úspěchu podnikání firmy.

Naši pracovníci		
Částečně něco vím	(17 / 23)	73 %
Ano, jsem se strategií/cíli dosti dobře seznámen/a	(5 / 23)	21 %
Podílím se na tvorbě firemní strategie	(1 / 23)	4 %

Pracovníci ostatních firem		
Částečně něco vím	(1853 / 4127)	44 %
Ano, jsem se strategií/cíli dosti dobře seznámen/a	(1338 / 4127)	32 %
Ne, o strategii a cílech firmy nevím nic	(526 / 4127)	12 %

Znalost informační strategie Informační strategie je částí podnikové strategie. Vychází z ní, a snaží zajistit co nejlepší podporu podnikových procesů pomocí informačních systémů. Znalost informační strategie není vyžadována u pracovníků firmy, ale je nutná u manažerů. Pracovníci firmy by však měli být rámcově informováni o cílech firmy v oblasti informačních systémů, jaké a kdy se plánují inovace či změny atp.

Naši pracovníci		
Ne, žádné	(11 / 23)	47 %
Ano, částečně	(11 / 23)	47 %
Ano	(1 / 23)	4 %

Pracovníci ostatních firem		
Ano, částečně	(1615 / 4125)	39 %
Ne, žádné	(1588 / 4125)	38 %
Podílím se na tvorbě informační strategie	(464 / 4125)	11 %

Informovanost o plnění cílů firmy Zde se zkoumá odpověď na otázku, zda nadřízení pravidelně informují své pracovníky o plnění strategických cílů firmy. Může se zdát, že tyto informace nejsou pro pracovníky důležité, ale zpravidla zvyšují pocit sounáležitosti pracovníků s firmou a mohou motivovat pracovníky. Pracovníci také mají pocit, že jsou pro podnik důležití a podnik vnímá jejich přínos pro ni.

Naši pracovníci		
Pravidelně	(11 / 23)	47 %
Občas	(7 / 23)	30 %
Nikdy	(3 / 23)	13 %
Pracovníci ostatních firem		
Občas	(1764 / 4127)	42 %
Pravidelně	(1342 / 4127)	32 %
Podílím se na vyhodnocování plnění strategických cílů firmy	(554 / 4127)	13 %

Informovanost o přispění pracovníka k dosaženým výsledkům firmy Tento bod je dost důležitý. Pokud pracovník neví, jak jeho práce přispívá k dosažení cílů firmy, jak je jeho práce významná pro podnik a tedy ani jak by mohl svojí prací zlepšovat dosahování podnikových cílů, vede to zpravidla k nižší efektivnost činnosti firmy.

Naši pracovníci		
Pravidelně	(12 / 23)	52 %
Občas	(5 / 23)	21 %
Ne	(5 / 23)	21 %
Pracovníci ostatních firem		
Občas	(1610 / 4125)	28 %
Pravidelně	(1451 / 4125)	35 %
Ne	(843 / 4125)	20 %

Pravidla pro práci s informačním systémem Zkoumá se, zda jsou v posuzovaném podniku stanovena jasná pravidla, za jaká data pracovníci zodpovídají, která data a kdy musí vkládat do systému a aktualizovat, jaké funkce informačního systému a kdy mají používat.

Naši pracovníci		
Ano, existují, ale nejsou příliš kontrolována nebo vyžadována	(8 / 23)	34 %
Ano, existují, a jsou velmi tvrdě vyžadována a kontrolována	(7 / 23)	30 %
Nemáme žádná pravidla, nebo o nich nevím	(5 / 23)	21 %
Pracovníci ostatních firem		
Ano, existují, ale nejsou příliš kontrolována nebo vyžadována	(343 / 867)	39 %
Ano, existují, a jsou velmi tvrdě vyžadována a kontrolována	(248 / 867)	28 %
Nemáme žádná pravidla, nebo o nich nevím	(176 / 867)	20 %

Efektivnost informačního systému

Tato kapitola zkoumá, jak jsou posuzované informační systémy efektivní, zda jsou vynaložené prostředky adekvátní výsledku a v jakých oblastech by mohl informační systém našim pracovníkům více pomáhat.

Mohli by naši pracovníci vykonávat svoji práci bez posuzovaného informačního systému? V tomto odstavci se zkoumá, jak je informační systém důležitý pro tamější pracovníky. Od této otázky se odvíjí i některá doporučení systému.

Naši pracovníci		
Rozhodně ne	(21 / 23)	91 %
Ano, s malými obtížemi	(1 / 23)	4 %
Částečně, s velkými obtížemi	(1 / 23)	4 %
Pracovníci ostatních firem		
Rozhodně ne	(2094 / 4158)	50 %
Částečně, s velkými obtížemi	(1417 / 4158)	34 %
Ano, s malými obtížemi	(473 / 4158)	11 %

Mohl by podnik fungovat bez posuzovaného informačního systému? Zde se zkoumá, jak je informační systém důležitý pro posuzování podniku, zda by bez něj mohla fungovat či nikoli.

Naši pracovníci		
Ne, v žádném případě	(20 / 23)	86 %
Ano, s většími problémy	(3 / 23)	13 %
Pracovníci ostatních firem		
Ne, v žádném případě	(2543 / 4151)	61 %
Ano, s většími problémy	(1204 / 4151)	29 %
Ano, bez větších problémů	(256 / 4151)	6 %

Mohl by informační systém více pomáhat tamějším pracovníkům a zlepšit tak procesy? V tomto bodě se zamýšlí naši pracovníci nad tím, zda by nějaká změna (či výměna posuzovaného informačního systému za jiný) zlepšila jejich práci. Odpovědi ukazují, do jaké míry je posuzovaný informační systém ve shodě s potřebami naši pracovníků.

Naši pracovníci		
Ano, zlepšilo by to částečně můj pracovní výkon (produktivitu práce)	(8 / 23)	34 %
Ano, zlepšilo by to informace, které potřebuji pro rozhodování	(7 / 23)	30 %
Ano, zlepšilo by to významně můj pracovní výkon (produktivitu práce)	(4 / 23)	17 %
Nevím	(2 / 23)	8 %
Pracovníci ostatních firem		
Ano, zlepšilo by to částečně můj pracovní výkon (produktivitu práce)	(1697 / 4150)	40 %
Ano, zlepšilo by to informace, které potřebuji pro rozhodování	(848 / 4150)	20 %
Ano, zlepšilo by to významně můj pracovní výkon (produktivitu práce)	(697 / 4150)	16 %
Nevím	(492 / 4150)	11 %

Školení pracovníků Tento bod zkoumá, zda naši pracovníci byli vyškoleni pro práci s posuzovaným informačním systémem. Z výzkumů vyplývá, že jen u malé části pracovníků nebylo školení přínosem, je proto velmi školení pořádat. Vede to vždy k zvýšení produktivity práce a menším nárokům na podporu pracovníků.

Naši pracovníci		
Ano, absolvoval/a	(21 / 23)	91 %
Ne, neabsolovoval/a a nebylo mi nabídnuto	(1 / 23)	4 %
Ne, neabsolvoval/a, ale bylo mi nabídnuto	(1 / 23)	4 %
Pracovníci ostatních firem		
Ano, absolvoval/a	(2353 / 4121)	57 %
Ne, neabsolovoval/a a nebylo mi nabídnuto	(1176 / 4121)	28 %
Ne, neabsolvoval/a, ale bylo mi nabídnuto	(592 / 4121)	14 %

Přínos školení pro pracovníky Zde se ukazuje, jaký byl přínos školení na informační systém pro pracovníky, kteří měli možnost se jej zúčastnit.

Naši pracovníci		
Ano, částečně	(14 / 23)	60 %
Ano	(6 / 23)	26 %
Nevím	(1 / 23)	4 %
Ne	(1 / 23)	4 %

Pracovníci ostatních firem		
Neabsolvoval/a jsem školení	(1397 / 4129)	33 %
Ano, částečně	(1230 / 4129)	29 %
Ano	(1225 / 4129)	29 %
Ne	(184 / 4129)	4 %

Potřebnost školení pro pracovníky Zde se zkoumá, jaký zájem mají naši pracovníci o možné školení na práci s informačním systémem. Pokud je zájem kladný, mohlo by uspořádání školení vést k zvýšení efektivnosti využívání systému.

Naši pracovníci		
Určitě ano	(9 / 23)	39 %
Spíše ano	(9 / 23)	39 %
Spíše ne	(3 / 23)	13 %
Pracovníci ostatních firem		
Spíše ano	(976 / 2671)	36 %
Ne, nepotřebuji ho	(587 / 2671)	21 %
Spíše ne	(564 / 2671)	21 %

Bezpečnost informačního systému

Tato kapitola zkoumá, zda naši pracovníci chápou informační systém jako službu, podpůrný proces své práce, nebo jako integrální součást svých procesů. Toto chápání je důležité pro úvahy o možném outsourcingu informačního systému, jeho části či podpory pracovníků.

Pravidla pro bezpečnost informačního systému Zkoumá se, zda jsou v posuzovaném podniku stanovena jasná bezpečnostní pravidla a zda je pracovníci dodržují a manažeři toto důsledně vyžadují.

Naši pracovníci		
Nemáme žádná pravidla, nebo o nich nevím	(8 / 23)	34 %
Ano, existují, ale nejsou příliš kontrolována nebo vyžadována	(7 / 23)	30 %
Ano, existují, a jsou velmi tvrdě vyžadována a kontrolována	(5 / 23)	21 %
Pracovníci ostatních firem		
Ano, existují, ale nejsou příliš kontrolována nebo vyžadována	(304 / 865)	35 %
Ano, existují, a jsou velmi tvrdě vyžadována a kontrolována	(281 / 865)	32 %
Nemáme žádná pravidla, nebo o nich nevím	(187 / 865)	21 %

Přístup do počítačové sítě - možná ohrožení Zkoumá se, zda si mohou naši pracovníci připojovat svoje soukromá přenosná zařízení do podnikové sítě. Riziko spočívá v možném nízkém zabezpečení těchto zařízení a umožnění případného útoku na naši síť viry, špionážními programy a podobně.

Naši pracovníci		
Nevím, nikdy jsem to nepotřeboval	(14 / 23)	60 %
Ano, není problém se připojit	(4 / 23)	17 %
Ne, firemní politika to zakazuje	(3 / 23)	13 %
Pracovníci ostatních firem		
Ne, firemní politika to zakazuje	(1018 / 2669)	38 %
Nevím, nikdy jsem to nepotřeboval	(737 / 2669)	27 %
Ano, není problém se připojit	(562 / 2669)	21 %

Přístup do počítačové sítě veřejností - možná ohrožení Zkoumá se, zda si mohou návštěvy, tedy cizí osoby v posuzovaném podniku, připojovat svoje zařízení do podnikové sítě. Riziko spočívá v možném nízkém zabezpečení těchto zařízení a umožnění případného útoku na naši síť viry, špionážními programy a podobně.

Naši pracovníci		
Nevím, nikdy to nebylo potřeba	(14 / 23)	60 %
Ano, pro tyto účely máme vyhrazenu bezdrátovou síť, bez přístupu do firemní sítě	(6 / 23)	26 %
Ne, firemní politika to zakazuje	(2 / 23)	8 %
Pracovníci ostatních firem		
Ne, firemní politika to zakazuje	(336 / 871)	38 %
Ano, pro tyto účely máme vyhrazenu bezdrátovou síť, bez přístupu do firemní sítě	(256 / 871)	29 %
Nevím, nikdy to nebylo potřeba	(181 / 871)	20 %

Zálohování dat Zde se zkoumá, zda mají naši pracovníci na svých počítačích uložena data a jak jsou chráněna proti případnému poškození nebo zničení.

Naši pracovníci		
Zálohování mého počítače probíhá automaticky	(13 / 23)	56 %
Pracovník útvaru informačních systémů nebo podpory informačních systémů	(5 / 23)	21 %
Já sám	(3 / 23)	13 %

Pracovníci ostatních firem		
Zálohování mého počítače probíhá automaticky	(979 / 2668)	36 %
Já sám	(849 / 2668)	31 %
Pracovník útvaru informačních systémů nebo podpory informačních systémů	(389 / 2668)	14 %

Dopad poškození dat Zjišťuje se, jaký je dopad zničení dat uložených na počítačích tamějších pracovníků. Jaká je četnost záloh a kolik času si vyžádá doplnění ztracených dat.

Naši pracovníci		
Žádné, všechna má data jsou mimo můj počítač	(6 / 23)	26 %
Méně než 1 den	(4 / 23)	17 %
Méně než 4 hodiny	(3 / 23)	13 %

Pracovníci ostatních firem		
Žádné, všechna má data jsou mimo můj počítač	(711 / 2665)	26 %
Méně než 1 den	(482 / 2665)	18 %
1-2 dny	(362 / 2665)	13 %

Dopad ztráty dat a jejich možné zneužití Zjišťuje se, jaký je dopad ztráty dat na počítačích pracovníků. Testuje se, jak vnímají naši pracovníci hrozbu ztráty dat.

Naši pracovníci		
Žádný, data na počítači jsou chráněna přihlašovacím jménem a heslem	(8 / 23)	34 %
Žádný, nemám na svém počítači žádná firemní data, všechno je mimo můj počítač	(6 / 23)	26 %
Střední, prozrazení firemních dat na tomto počítači může firmě způsobit problémy	(4 / 23)	17 %

Pracovníci ostatních firem		
Žádný, data na počítači jsou chráněna přihlašovacím jménem a heslem	(868 / 2665)	32 %
Žádný, nemám na svém počítači žádná firemní data, všechno je mimo můj počítač	(552 / 2665)	20 %
Mírný, prozrazení firemních dat na tomto počítači nemůže firmě způsobit vážnější problémy	(517 / 2665)	19 %

Úroveň vnímání rizik u pracovníků Testuje se citlivost pracovníků při ohrožení bezpečnost jejich počítače. Zjišťuje se, jak by pracovníci reagovali v případě možného ohrožení jejich počítače útočícím virem, špionážním programem či podobnou závadnou aplikací. Naši pracovníci by na žádost o povolení přístupu neznámého programu na jejich počítač (byť se tvářícího neškodně a legitimně) reagovali následovně:

Naši pracovníci		
Ne, odmítl bych	(17 / 23)	73 %
Ano, povolil bych, ale napřed bych si vyžádal souhlas svého nadřízeného	(3 / 23)	13 %
Okamžitě bych zavřel okno prohlížeče a ohlásil možný bezpečnostní incident nadřízenému	(2 / 23)	8 %
Pracovníci ostatních firem		
Ne, odmítl bych	(1618 / 2671)	60 %
Ano, povolil bych, ale napřed bych si vyžádal souhlas svého nadřízeného	(324 / 2671)	12 %
Okamžitě bych zavřel okno prohlížeče a ohlásil možný bezpečnostní incident nadřízenému	(303 / 2671)	11 %

Vnímání důležitosti bezpečnostní politiky Zjišťuje se, jaký mají vztah naši pracovníci k bezpečnosti v oblasti informačních systémů na otázce, jak chrání svoje přístupová hesla.

Naši pracovníci		
Pamatuji si je	(18 / 23)	78 %
Mám je zapsaná někde poblíž počítače	(4 / 23)	17 %
Mám je uložena ve speciální aplikaci	(1 / 23)	4 %
Pracovníci ostatních firem		
Pamatuji si je	(1854 / 2670)	69 %
Mám je zapsaná někde poblíž počítače	(363 / 2670)	13 %
Mám je uložena ve speciální aplikaci	(337 / 2670)	12 %

Přístup na internet a zranitelnost systému Ověřuje se, zda mají naši pracovníci přístup na internet. U některých profesí je tento přístup nutný, ale zároveň počítače těchto pracovníků musí být dobře chráněny proti možným (a pravděpodobným) útokům.

Naši pracovníci		
Ano, bez omezení	(21 / 23)	91 %
Částečně, pouze na vybrané stránky	(2 / 23)	8 %
Pracovníci ostatních firem		
Ano, bez omezení	(1765 / 2668)	66 %
Částečně, pouze na vybrané stránky	(783 / 266)	29 %
Ne	(120 / 2668)	4 %

Riziko zneužití dat a ohrožení bezpečnosti Zjišťuje se, zda si naši pracovníci mohou připojit k počítači externí paměťová média (disky, flash paměti) a kopírovat a odnášet

tak případně firemní data, případně infikovat počítače posuzovaného podniku závadnými programy.

Naši pracovníci		
Ano	(18 / 23)	78 %
Nevím	(5 / 23)	21 %
Pracovníci ostatních firem		
Ano	(2248 / 2668)	84 %
Ne	(262 / 2668)	9 %
Nevím	(158 / 2668)	5 %

Riziko instalace programů uživateli V této subkapitole se ověřuje, zda mohou uživatelé IS instalovat sami programy na počítače v podniku. Jde o velké bezpečnostní a trestně právní riziko. Pokud uživatel nainstaluje nelegální programy, odpovědnost je i na straně podniku.

Naši pracovníci		
Ano	(11 / 23)	47 %
Ano, se svolením nadřízeného	(6 / 23)	26 %
Ne	(6 / 23)	26 %
Pracovníci ostatních firem		
Ne	(1254 / 2670)	46 %
Ano	(785 / 2670)	29 %
Ano, se svolením nadřízeného	(387 / 2670)	14 %

Chápání informačních systémů jako služby

Tato kapitola zkoumá, zda naši pracovníci chápou informační systém jako službu, podpůrný proces své práce, nebo jako integrální součást svých procesů. Toto chápání je důležité pro úvahy o možném outsourcingu informačního systému, jeho části či podpory pracovníků.

Vnímání informačního systému jako externí služby V této otázce se zkoumá, zda naši pracovníci chápou informační systém jako službu, kterou by bylo možnost zajišťovat i externí formou, tedy neprovozovat systém v posuzovaném podniku, ale pronajímat si jej od nějakého dodavatele.

Naši pracovníci		
Nevím	(7 / 23)	30 %
Spíše ne	(6 / 23)	26 %
Spíše ano	(5 / 23)	21 %

Pracovníci ostatních firem		
Spíše ne	(1217 / 4117)	29 %
Nevím	(1011 / 4117)	24 %
Určitě ne	(839 / 4117)	20 %

Využívání outsourcingu v informačních systémech posuzovaného podniku Zde se zjišťuje, zda a v jaké míře posuzovaná podnik využívá outsourcing v oblasti informačního systému nebo jeho podpory. Outsourcing je chápan ve smyslu externího zajištění, nezkoumá se, zda před tím podnik tento proces vlastnil a převedl jej na externího dodavatele.

Naši pracovníci		
Nevím	(14 / 23)	60 %
Hodně, pro celý systém nebo převažující část	(4 / 23)	17 %
Ne	(3 / 23)	13 %

Pracovníci ostatních firem		
Ne	(750 / 1712)	43 %
Málo, pouze pro malou část informačního systému	(438 / 1712)	25 %
Nevím	(372 / 1712)	21 %

Zkušenosti s outsourcingem V tomto bodě se zjišťují zkušenosti pracovníků s outsourcingem.

Naši pracovníci		
Žádné zkušenosti nemám	(16 / 23)	60 %
Spíše pozitivní	(7 / 23)	30 %

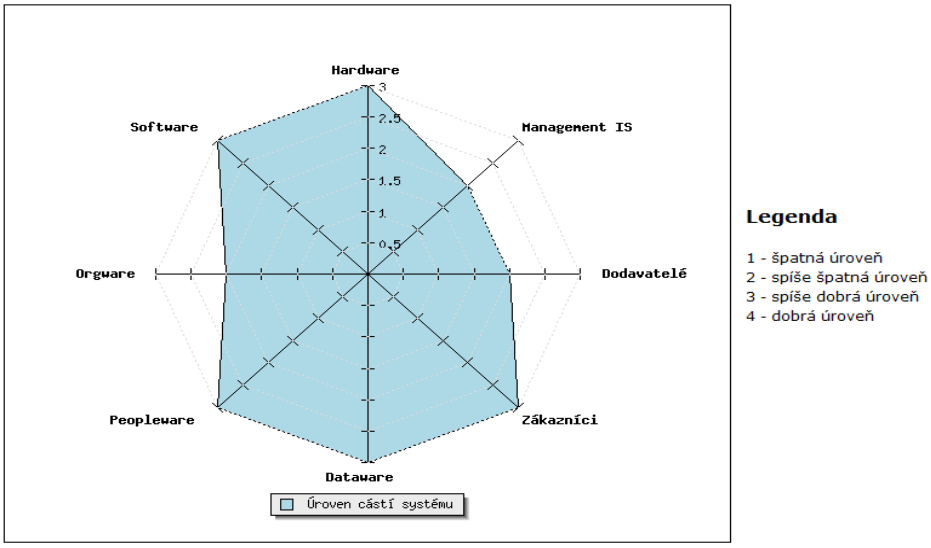
Pracovníci ostatních firem		
Žádné zkušenosti nemám	(2659 / 4117)	64 %
Spíše pozitivní	(824 / 4117)	20 %
Spíše negativní	(348 / 4117)	8 %

A.1.2 Ohodnocení jednotlivých částí informačního systému HOS

Posouzení zkoumaných oblastí

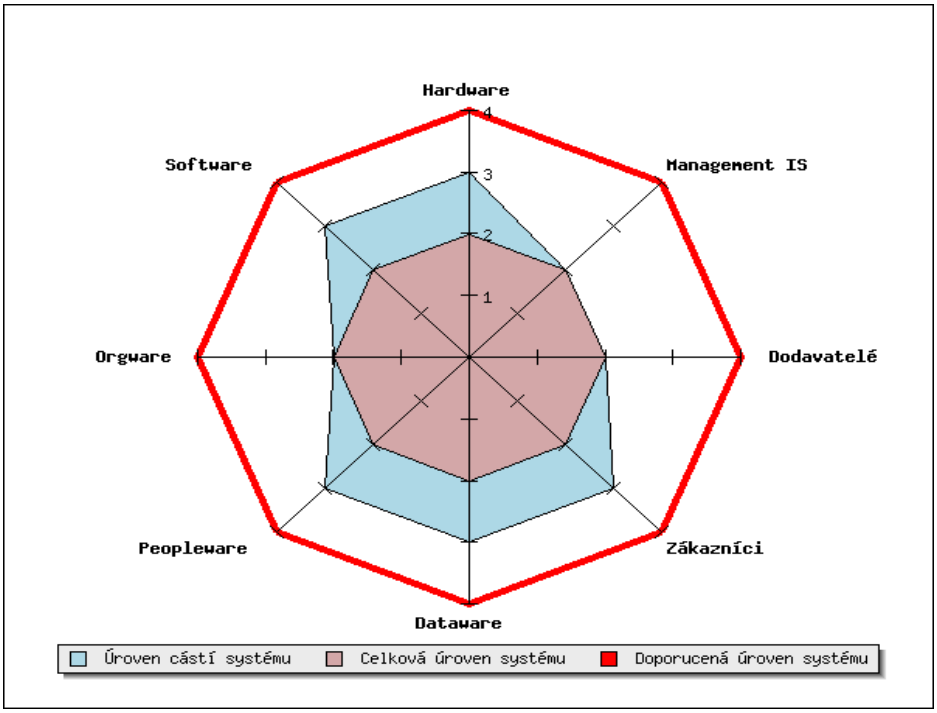
Hadrware	3	spíše dobrá úroveň
Software	3	spíše dobrá úroveň
Orgware	2	spíše špatná úroveň
Peopleware	3	spíše dobrá úroveň
Dataware	3	spíše dobrá úroveň
Dataware	3	spíše dobrá úroveň
Zákazníci	3	spíše dobrá úroveň
Dodavatelé	2	spíše špatná úroveň
Management IS	2	spíše špatná úroveň

Tabulka A.1: Metoda HOS8



Obrázek A.1: Úroveň posouzení zkoumaných objektů

Celkový stav posuzovaného systému



Obrázek A.2: Celková úroveň informačního systému: 2 (spíše špatná úroveň)

Doporučená úroveň informačního systému je znázorněna červeným osmiúhelníkem v grafu. Celková úroveň informačního systému je znázorněna růžovou oblastí v grafu.

Vyhodnocení

Posuzovaný systém je horší než je očekávaná úroveň, daná důležitostí systému pro podnik, v oblastech:

- **Hardware**
- **Software**
- **Orgware**
- **Peopleware**
- **Dataware**
- **Zákazníci**
- **Dodavatelé**
- **Management IS**

Hardware

- Není vyloučeno, že technika neodpovídá výkonově potřebám systému, a je třeba ji posílit, inovovat.
- Bylo by dobré prověřit kvalitu počítačových sítí a jejich rychlost.
- Není dobré pořizovat nové technické vybavení bez ověření kompatibility se stávající technikou, může to způsobovat problémy ve výkonu celého systému.
- Je dobré mít záložní technické vybavení klíčových částí systému pro případ havárie.
- Technika bude zřejmě již pomalu potřebovat obměnu, zdá se být dosti stará.

Software

- Při výběru informačního systému je třeba předem stanovit, které funkce jsou požadovány. Zdá se, že Váš systém neobsahuje všechny důležité funkce potřebné pro jeho uživatele.
- Práce s informačním systémem není pro uživatele asi příliš snadná, stojí za zvážení úprava komunikačního prostředí systému - jednotný, jasný, přehledný styl.
- Chybová hlášení posuzovaného systému by měla být více srozumitelná uživatelům.
- Posuzovaný informační systém se nezdá být příliš dobrý, spokojenost s ním je dosti malá.

Orgware

- Je velmi žádoucí mít definované postupy a směrnice pro řešení havarijních stavů systémů.
- Je velmi žádoucí mít pracovní postupy a předpisy pro práci s informačním systémem pro koncové uživatele a udržovat je v aktuálním stavu.
- Je velmi žádoucí mít v podniku bezpečnostní pravidla informačního systému a udržovat je aktuální.
- Zdá se, že management příliš nekontroluje dodržování pravidel bezpečnosti a provozu informačních systémů. To může být způsobit vážné problémy.
- Každý pracovník by měl mít jasně určeno, s jakými úlohami (funkcemi informačního systému) smí či musí pracovat a kdy.
- Uživatelé by neměli mít možnost instalovat na své počítače nové programy, měnit nastavení a připojovat zařízení k počítači.
- Je třeba správně a včas zrušit přístupová práva k informačnímu systému zaměstnancům, kteří ukončí pracovní poměr.
- Pravidla pro provoz a bezpečnost informačního systému by měla vždy existovat, být jasná a logická.

Peopleware

- Měla by probíhat školení pracovníků na práci s informačním systémem a na pravidla bezpečnosti.
- Je vhodné mít zastupitelnost klíčových pracovníků při práci s informačním systémem.
- Je zřejmě třeba zvýšit důraz na dodržování pravidel a trestat jejich porušování.
- Je na zvážení, zda více nepodporovat další vzdělávání pracovníků, případně školení na informační systém.

Dataware

- Pracovníci by měli mít jasně vymezenou odpovědnost za data, která spravují.
- Je velmi žádoucí mít přesně stanovená pravidla, kdo a kdy musí jaká data vložit do informačního systému.
- Zdá se, že pracovníci nemají k dispozici všechna data, která by potřebovali ke své práci.

- Uživatelé by neměli získávat nepřesná a nadbytečná data.
- Zdá se, že v posuzovaném podniku neprobíhá pravidelné zálohování dat na počítačích uživatelů. To může přinášet i vážné problémy.
- Měly by existovat plány obnovy dat ze záloh v případě havárie systému.
- Média se zálohami by měla být katalogizována a dobře chráněna před poškození a zneužitím.

Zákazníci

- Měly by být jasně definovány cíle informačního systému vzhledem k jeho zákazníkům (uživatelům).
- Měly by být jasně definovány metriky informačního systému vzhledem k jeho zákazníkům (uživatelům) - tedy ukazatele, kterými se měří, jak informační systém plní vůči zákazníkům svoji roli, jak jsou s ním spokojeni atp., a měly by být pravidelně vyhodnocovány.
- Mělo by být pravidelně zkoumáno, jaké přínosy od posuzovaného informačního systému zákazníci očekávají.
- Výstupy z informačního systému pro zákazníky by měly být customizovány, tedy konkrétní zákazním by měl dostávat i informace určené přímo pro něj.
- Rychlost odezvy informačního systému pro zákazníky není zřejmě dostatečně dobrá.
- Bylo by dobré zlepšit ochranu citlivých obchodních dat o zákaznících.
- Systém určený pro zákazníky by měl nabízet i alternativní přístup k informacím, například pomocí RSS, sociálních sítí, SMS a podobně.

Dodavatelé

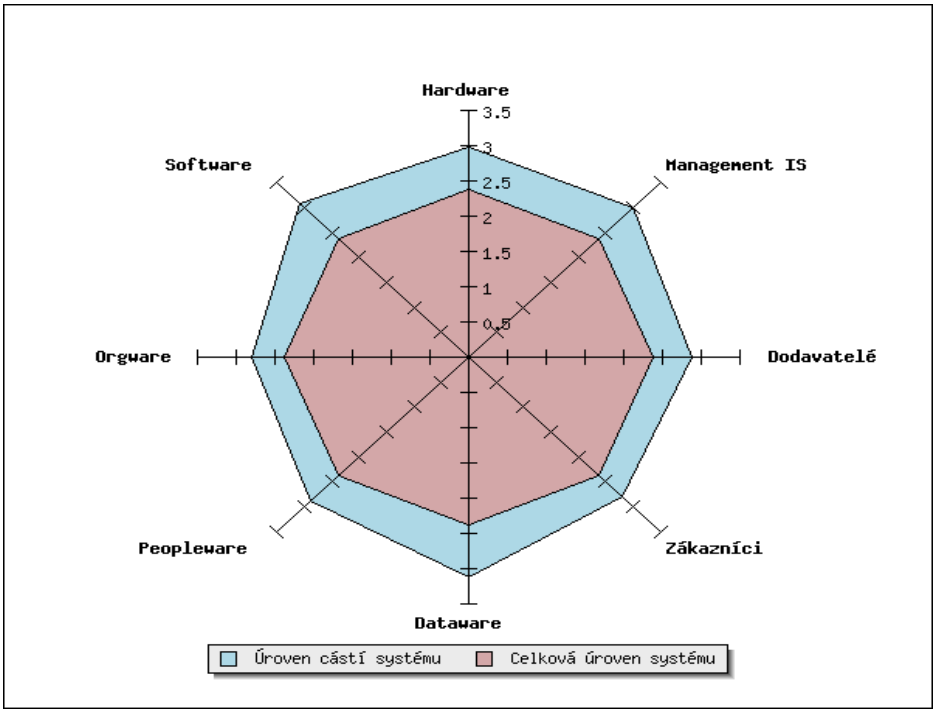
- Zdá se, že posuzovaný podnik nevyužívá SLA (service level agreement, dohoda o úrovni poskytované služby) s dodavatelem informačního systému (tím, kdo pro nás zajišťuje jeho provoz). Neexistence jasně stanovených pravidel je jedním z hlavním zdrojů neefektivnosti informačního systému.
- Bez uplatňování sankcí za nedodržení pravidel provozování informačního systému ztrácí SLA (pravidla za jakých je IS provozován, dodáván) účinnost.
- Bylo by asi třeba zlepšit technickou podporu (opravy počítačů, výměny tonerů v tiskárnách atp.) pracovníků.

- Bylo by asi třeba zlepšit uživatelskou podporu (rady a pomoc při práci s informačním systémem).
- Zdá se, že dodavatel (provozovatel) informačního systému nevyhovuje našim potřebám.
- Je nutné mít u zřízen tzv. service desk, kontaktní místo pro hlášení požadavků na podporu při práci s informačním systémem.
- Zdá se, že posuzovaný dodavatel (provozovatel) informačního systému o nás jako zákazníka nejeví příliš velký zájem.

Management IS

- Manažeři by měli striktně trvat na dodržování všech existujících pravidel provozu a bezpečnosti informačního systému a kontrolovat jejich dodržování.
- Bylo by dobré poskytovat dodavateli (provozovateli) informačního systému zpětnou vazbu, jak jsme s jeho prací spokojeni, co nového případně potřebujeme.
- Pokud posuzovaný podnik nemá informační strategii (plán, jak bude vypadat posuzovaný informační systém, jak podporuje naši podnikovou strategii), pak nelze zkoumat efektivnost takového systému, protože není definováno, jaké cíle má plnit. Obvykle to způsobuje vysoké neřízené náklady.
- Zdá se, že management firmy si dostatečně neuvědomuje potenciál a význam informačních systémů pro činnost a rozvoj firmy.
- Management možná ne dostatečně doceňuje význam koncových uživatelů pro správnou činnost informačního systému.
- Hlavní manažer firmy (CIO) buď v posuzovaném podniku neexistuje, nebo nejeví dostatečný zájem o rozvoj informačních systémů.

Srovnání stavu informačního systému



Obrázek A.3: Srovnání všech podniků (celkem 282 podniků)

A.2 Ohodnocení aktiv

Hodnocení důležitosti	**Úroveň**
IS nemůže bez aktiva fungovat	5
IS bez aktiva může jen stěží fungovat	4
IS bez aktiva může fungovat, ale s obtížemi	3
Aktivum usnadňuje práci s IS, avšak není pro něj důležité	2
Aktivum je pro IS z hlediska funkčnosti zanedbatelný	1

Tabulka A.2: Stupnice důležitosti aktiv z hlediska IS

Hodnocení integrity	**Úroveň**
Zcela propojené s IS	5
Vysoké propojení s IS	4
Podpůrná integrace s IS	3
Nízká integrace s IS	2
Integrace s IS velmi nízká nebo neexistuje	1

Tabulka A.3: Stupnice integrace aktiv s IS

Hodnocení finanční ztráty	**Úroveň**
Kritické ztráty	5
Značné ztráty	4
Ztráty do výše hranice únosnosti	3
Nízké ztráty	2
Zanedbatelné ztráty	1

Tabulka A.4: Stupnice finanční ztráty z aktiv

A.3 Ohodnocení hrozeb

Pravděpodobnost vzniku hrozby	**Úroveň**
Velmi vysoká	5
Vysoká	4
Střední	3
Nízká	2
Žádná	1

Tabulka A.5: Stupnice pravděpodobnosti vzniku hrozby

Zranitelnost aktiva	**Úroveň**
Hrozba může poškodit aktivum do velmi vysoké míry	5
Míra poškození hrozbou na nebezpečné úrovni	4
Aktivum je hrozbou ohroženo na hranici únosnosti	3
Ohrožení aktiva hrozbou na nízké úrovni	2
Zanedbatelné ohrožení aktiva danou hrozbou	1

Tabulka A.6: Stupnice zranitelnosti aktiva

A.4 Hranice přijatelnosti rizik

Interval v %	**Hranice přijatelnosti rizika**
(00 - 34>	Nízké riziko
(34 - 68>	Střední riziko
(68 - 100)	Vysoké riziko

Tabulka A.7: Hranice přijatelnosti rizik

A.5 Odhad ceny ztracených dat

Výpočet hodnoty dat je založen na počtu 13000 záznamů, složených ze záznamů dodavatelů, odběratelů a zaměstnanců.

Internal Investigation	-20%	Average Cost	+20%
Cybercrime consulting	71760	89700	107640
Attorney fees	72758.4	90948	109137.6
Sum:	$ 144518	$ 180648	$ 216778
Notification/Crisis Management			
Customer notification (certified mail)	132288	165360	198432
Call center support	93600	117000	140400
Crisis management consulting	52416	65520	78624
Media management	10358.4	12948	15537.6
Sum:	$ 288662	$ 360828	$ 432994
Regulatory/Compliance			
Credit monitoring for affected customers	601536	751920	902304
Regulatory investigation defense	222518.4	278148	333777.6
State/Federal fines or fees	471993.6	589992	707990.4
Sum:	$ 1296048	$ 1620060	$ 1944072
Total Data Loss Expenses:	$ 1729228	$ 2161536	$ 2593844

Obrázek A.4: Odhad hodnoty podnikových dat (38)

A.6 Potřebné údaje pro zhodnocení investic

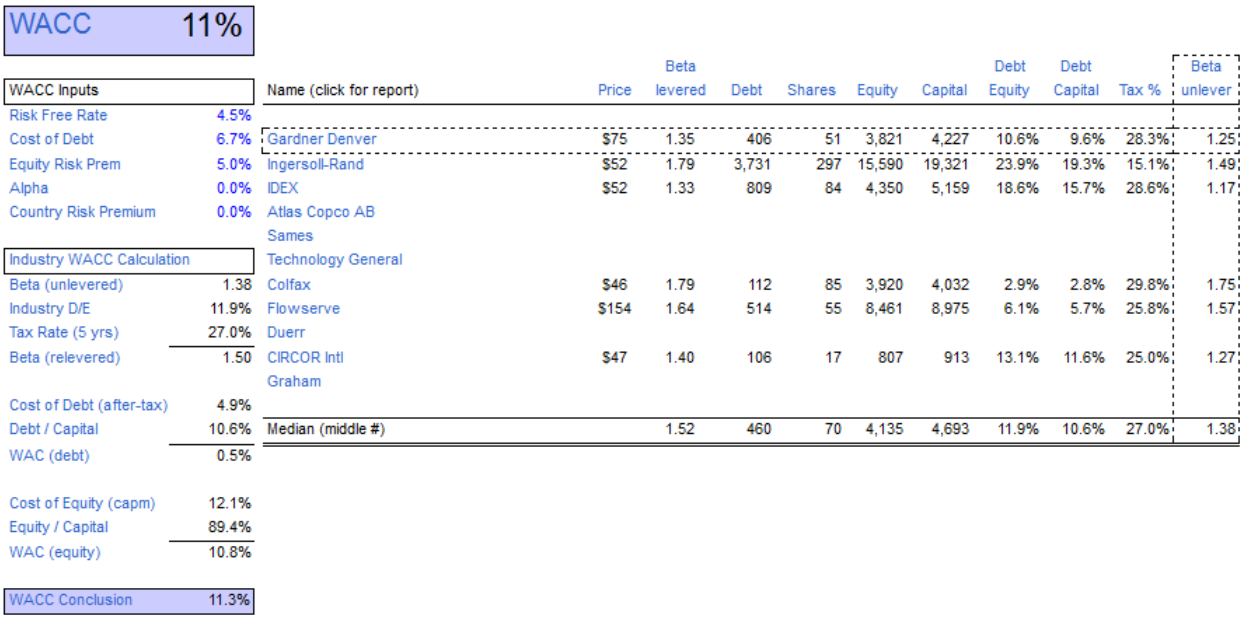
Years ended December 31
(Dollars in thousands)

	2011	2010	2009
Cash flows from operating activities:			
Net income (loss)	**$ 279,542**	174,954	(163,299)
Adjustments to reconcile net income (loss) to net cash provided by operating activities:			
Depreciation and amortization	**60,284**	60,248	68,731
Impairment charges	**—**	—	262,400
Foreign currency transaction (gain) loss, net	**(684)**	(2,047)	457
Net loss on asset dispositions	**1,944**	2,114	1,255
LIFO liquidation income	**(204)**	(754)	(297)
Stock issued for employee benefit plans	**1,138**	3,719	3,954
Stock-based compensation expense	**6,453**	6,398	2,980
Excess tax benefits from stock-based compensation	**(3,396)**	(3,195)	(479)
Deferred income taxes	**(10,574)**	(8,756)	(8,227)
Changes in assets and liabilities:			
Receivables	**(88,380)**	(43,845)	72,056
Inventories	**(46,374)**	(15,418)	67,498
Accounts payable and accrued liabilities	**88,933**	36,705	(89,918)
Other assets and liabilities, net	**11,129**	(7,875)	(5,800)
Net cash provided by operating activities	**299,811**	202,248	211,311
Cash flows from investing activities:			
Capital expenditures	**(55,688)**	(33,039)	(42,766)
Net cash paid in business combinations	**(196,373)**	(12,142)	(81)
Disposals of property, plant and equipment	**3,735**	2,681	1,187
Other	**—**	—	(2)
Net cash used in investing activities	**(248,326)**	(42,500)	(41,662)
Cash flows from financing activities:			
Principal payments on short-term borrowings	**(18,496)**	(24,866)	(33,466)
Proceeds from short-term borrowings	**13,371**	26,913	25,018
Principal payments on long-term debt	**(330,108)**	(82,808)	(231,725)
Proceeds from long-term debt	**447,594**	8,034	52,169
Proceeds from stock option exercises	**7,514**	19,565	3,751
Excess tax benefits from stock-based compensation	**3,396**	3,195	479
Purchase of treasury stock	**(132,607)**	(49,400)	(867)
Debt issuance costs	**(599)**	—	(166)
Cash dividends paid	**(10,384)**	(10,499)	(2,608)
Purchase of shares from noncontrolling interests	**(18,806)**	—	—
Other	**(1,023)**	(992)	(760)
Net cash used in financing activities	**(40,148)**	(110,858)	(188,175)
Effect of exchange rate changes on cash and cash equivalents	**(13,107)**	(1,597)	7,527
(Decrease) increase in cash and cash equivalents	**(1,770)**	47,293	(10,999)
Cash and cash equivalents, beginning of year	**157,029**	109,736	120,735
Cash and cash equivalents, end of year	**$ 155,259**	157,029	109,736

Obrázek A.5: Peněžní roky v letech 2009-2011

Rok	2009	2010	2011	2012	2013
CF	109736	$157029	$155259	$186198	$195331
Rok	**2014**	**2015**	**2016**	**2017**	**2018**
CF	$219001	$232979	$253419	$269551	$288555

Tabulka A.8: Predikce peněžních toků v letech 2013-2017



WACC 11%

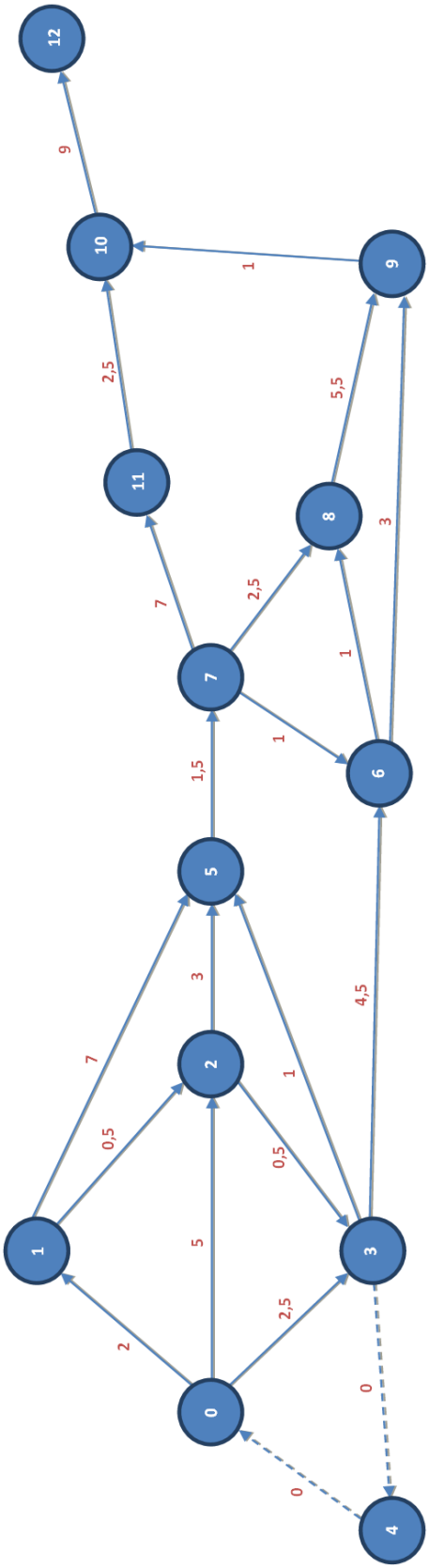
WACC Inputs	
Risk Free Rate	4.5%
Cost of Debt	6.7%
Equity Risk Prem	5.0%
Alpha	0.0%
Country Risk Premium	0.0%
Industry WACC Calculation	
Beta (unlevered)	1.38
Industry D/E	11.9%
Tax Rate (5 yrs)	27.0%
Beta (relevered)	1.50
Cost of Debt (after-tax)	4.9%
Debt / Capital	10.6%
WAC (debt)	0.5%
Cost of Equity (capm)	12.1%
Equity / Capital	89.4%
WAC (equity)	10.8%
WACC Conclusion	11.3%

Name (click for report)	Price	Beta levered	Debt	Shares	Equity	Capital	Debt Equity	Debt Capital	Tax %	Beta unlever
Gardner Denver	$75	1.35	406	51	3,821	4,227	10.6%	9.6%	28.3%	1.25
Ingersoll-Rand	$52	1.79	3,731	297	15,590	19,321	23.9%	19.3%	15.1%	1.49
IDEX	$52	1.33	809	84	4,350	5,159	18.6%	15.7%	28.6%	1.17
Atlas Copco AB										
Sames										
Technology General										
Colfax	$46	1.79	112	85	3,920	4,032	2.9%	2.8%	29.8%	1.75
Flowserve	$154	1.64	514	55	8,461	8,975	6.1%	5.7%	25.8%	1.57
Duerr										
CIRCOR Intl	$47	1.40	106	17	807	913	13.1%	11.6%	25.0%	1.27
Graham										
Median (middle #)		1.52	460	70	4,135	4,693	11.9%	10.6%	27.0%	1.38

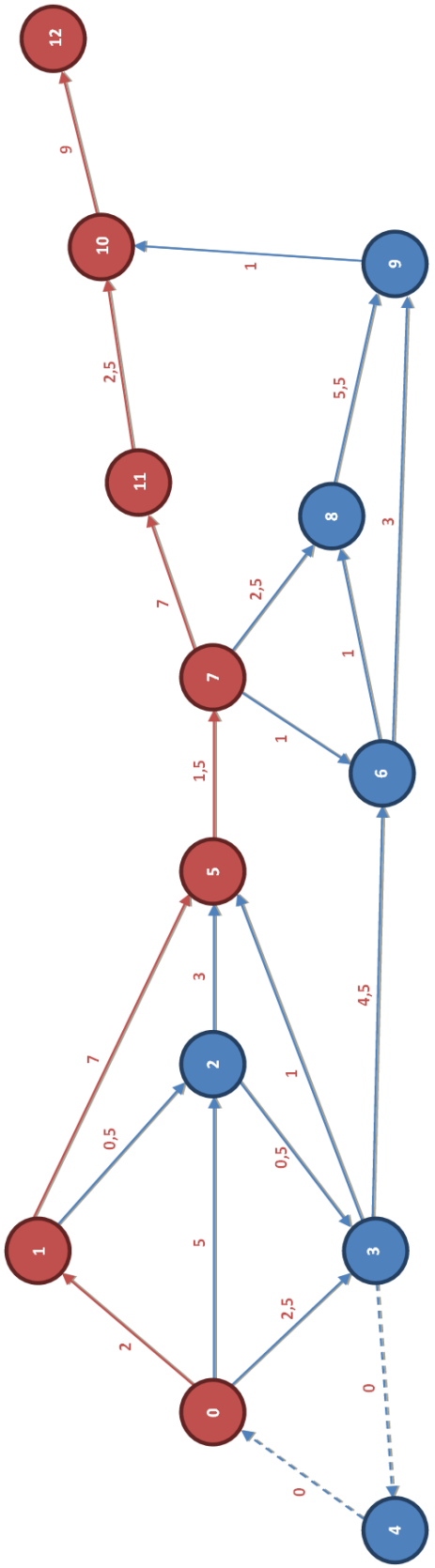
Obrázek A.6: Diskontní úroková míra

A.7 Stochastická metoda PERT

Obrázky dostupné na dalších stránkách.



Obrázek A.7: Řízení projektu pomocí metody PERT



Obrázek A.8: Kritická cesta v grafu PERT

A.8 Distribuční funkce

Pokud je distribuční funkce záporná, tak platí: $\phi(u) = 1 - \phi(u)$
Tabulky jsou uvedené na další stránkách.

u	$\phi(u)$	u	$\phi(u)$	u	$\phi(u)$	u	$\phi(u)$
0,00	0,50000	0,40	0,65542	0,80	0,78814	1,20	0,88493
0,01	0,50399	0,41	0,65910	0,81	0,79103	1,21	0,88686
0,02	0,50798	0,42	0,66276	0,82	0,79389	1,22	0,88877
0,03	0,51197	0,43	0,66640	0,83	0,79673	1,23	0,89065
0,04	0,51595	0,44	0,67003	0,84	0,79955	1,24	0,89251
0,05	0,51994	0,45	0,67364	0,85	0,80234	1,25	0,89435
0,06	0,52392	0,46	0,67724	0,86	0,80511	1,26	0,89617
0,07	0,52790	0,47	0,68082	0,87	0,80785	1,27	0,89796
0,08	0,53188	0,48	0,68439	0,88	0,81057	1,28	0,89973
0,09	0,53586	0,49	0,68793	0,89	0,81327	1,29	0,90147
0,10	0,53983	0,50	0,69146	0,90	0,81594	1,30	0,90320
0,11	0,54380	0,51	0,69497	0,91	0,81859	1,31	0,90490
0,12	0,54776	0,52	0,69847	0,92	0,82121	1,32	0,90658
0,13	0,55172	0,53	0,70194	0,93	0,82381	1,33	0,90824
0,14	0,55567	0,54	0,70540	0,94	0,82639	1,34	0,90988
0,15	0,55962	0,55	0,70884	0,95	0,82894	1,35	0,91149
0,16	0,56356	0,56	0,71226	0,96	0,83147	1,36	0,91309
0,17	0,56749	0,57	0,71566	0,97	0,83398	1,37	0,91466
0,18	0,57142	0,58	0,71904	0,98	0,83646	1,38	0,91621
0,19	0,57535	0,59	0,72240	0,99	0,83891	1,39	0,91774
0,20	0,57926	0,60	0,72575	1,00	0,84134	1,40	0,91924
0,21	0,58317	0,61	0,72907	1,01	0,84375	1,41	0,92073
0,22	0,58706	0,62	0,73237	1,02	0,84614	1,42	0,92220
0,23	0,59095	0,63	0,73565	1,03	0,84850	1,43	0,92364
0,24	0,59483	0,64	0,73891	1,04	0,85083	1,44	0,92507
0,25	0,59871	0,65	0,74215	1,05	0,85314	1,45	0,92647
0,26	0,60257	0,66	0,74537	1,06	0,85543	1,46	0,92786
0,27	0,60642	0,67	0,74857	1,07	0,85769	1,47	0,92922
0,28	0,61026	0,68	0,75175	1,08	0,85993	1,48	0,93056
0,29	0,61409	0,69	0,75490	1,09	0,86214	1,49	0,93189
0,30	0,61791	0,70	0,75804	1,10	0,86433	1,50	0,93319
0,31	0,62172	0,71	0,76115	1,11	0,86650	1,51	0,93448
0,32	0,62552	0,72	0,76424	1,12	0,86864	1,52	0,93574
0,33	0,62930	0,73	0,76730	1,13	0,87076	1,53	0,93699
0,34	0,63307	0,74	0,77035	1,14	0,87286	1,54	0,93822
0,35	0,63683	0,75	0,77377	1,15	0,87493	1,55	0,93943
0,36	0,64058	0,76	0,77637	1,16	0,87698	1,56	0,94062
0,37	0,64431	0,77	0,77935	1,17	0,87900	1,57	0,94179
0,38	0,64803	0,78	0,78230	1,18	0,88100	1,58	0,94295
0,39	0,65173	0,79	0,78524	1,19	0,88298	1,59	0,94408

Tabulka A.9: Hodnoty distribuční funkce normálního rozdělení N(0,1) I.část

u	$\phi(u)$	u	$\phi(u)$	u	$\phi(u)$	u	$\phi(u)$
1,60	0,94520	2,00	0,97725	2,40	0,99180	3,10	0,99903
1,61	0,94630	2,01	0,97778	2,41	0,99202	3,12	0,99910
1,62	0,94738	2,02	0,97831	2,42	0,99224	3,14	0,99916
1,63	0,94845	2,03	0,97882	2,43	0,99245	3,16	0,99921
1,64	0,94950	2,04	0,97932	2,44	0,99266	3,18	0,99926
1,65	0,95053	2,05	0,97982	2,45	0,99286	3,20	0,99931
1,66	0,95154	2,06	0,98030	2,46	0,99305	3,22	0,99936
1,67	0,95254	2,07	0,98077	2,47	0,99324	3,24	0,99940
1,68	0,95352	2,08	0,98124	2,48	0,99343	3,26	0,99944
1,69	0,95449	2,09	0,98169	2,49	0,99361	3,28	0,99948
1,70	0,95543	2,10	0,98214	2,50	0,99379	3,30	0,99952
1,71	0,95637	2,11	0,98257	2,52	0,99413	3,32	0,99955
1,72	0,95728	2,12	0,98300	2,54	0,99446	3,34	0,99958
1,73	0,95818	2,13	0,98341	2,56	0,99477	3,36	0,99961
1,74	0,95907	2,14	0,98382	2,58	0,99506	3,38	0,99964
1,75	0,95994	2,15	0,98422	2,60	0,99534	3,40	0,99966
1,76	0,96080	2,16	0,98461	2,62	0,99560	3,42	0,99969
1,77	0,96164	2,17	0,98500	2,64	0,99585	3,44	0,99971
1,78	0,96246	2,18	0,98537	2,66	0,99609	3,46	0,99973
1,79	0,96327	2,19	0,98574	2,68	0,99632	3,48	0,99975
1,80	0,96407	2,20	0,98610	2,70	0,99653	3,50	0,99977
1,81	0,96485	2,21	0,98645	2,72	0,99674	3,55	0,99981
1,82	0,96562	2,22	0,98679	2,74	0,99693	3,60	0,99984
1,83	0,96638	2,23	0,98713	2,76	0,99711	3,65	0,99987
1,84	0,96712	2,24	0,98745	2,78	0,99728	3,70	0,99989
1,85	0,96784	2,25	0,98778	2,80	0,99744	3,75	0,99991
1,86	0,96856	2,26	0,98809	2,82	0,99760	3,80	0,99993
1,87	0,96926	2,27	0,98840	2,84	0,99774	3,85	0,99994
1,88	0,96995	2,28	0,98870	2,86	0,99788	3,90	0,99995
1,89	0,97062	2,29	0,98899	2,88	0,99801	3,95	0,99996
1,90	0,97128	2,30	0,98928	2,90	0,99813	4,00	0,99997
1,91	0,97193	2,31	0,98956	2,92	0,99825	4,05	0,99997
1,92	0,97257	2,32	0,98983	2,94	0,99836	4,10	0,99998
1,93	0,97320	2,33	0,99010	2,96	0,99846	4,15	0,99998
1,94	0,97381	2,34	0,99036	2,98	0,99856	4,20	0,99999
1,95	0,97441	2,35	0,99061	3,00	0,99865	4,25	0,99999
1,96	0,97500	2,36	0,99086	3,02	0,99874	4,30	0,99999
1,97	0,97558	2,37	0,99111	3,04	0,99882	4,35	0,99999
1,98	0,97615	2,38	0,99134	3,06	0,99889	4,40	0,99999
1,99	0,97670	2,39	0,99158	3,08	0,99897	4,45	1,00000

Tabulka A.10: Hodnoty distribuční funkce normálního rozdělení N(0,1) II.část