VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

NÁVRH PROCESŮ PRO SPOLEČNOST POSKYTUJÍCÍ IT SLUŽBY S OHLEDEM NA ISMS A ITSM

DRAFT OF PROCESSES FOR IT OUTSOURCING COMPANY CONSIDERING ISMS AND ITSM

DIPLOMOVÁ PRÁCE

MASTER´S THESIS

AUTOR PRÁCE — BC. MARTIN HALLER

AUTHOR

VEDOUCÍ PRÁCE — ING. PETR SEDLÁK

SUPERVISOR

BRNO 2012

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2011/2012
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Haller Martin, Bc.

Informační management (6209T015)

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:

Návrh procesů pro společnost poskytující IT služby s ohledem na ISMS a ITSM

v anglickém jazyce:

Draft of Processes for IT Outsourcing Company Considering ISMS and ITSM

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Analýza současného stavu
Teoretická východiska řešení
Návrh řešení
Zhodnocení a závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

ČESKÝ NORMALIZAČNÍ INSTITUT. ČSN ISO/IEC 20000-2:2007. Informační technologie - Management služeb - Část 2: Soubor postupů. Praha: Český normalizační institut 2007.
ČESKÝ NORMALIZAČNÍ INSTITUT. ČSN ISO/IEC 27001:2006. Informační technologie - Bezpečnostní techniky - Systém managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut 2006.
ČESKÝ NORMALIZAČNÍ INSTITUT. ČSN ISO/IEC 27002:2008. Informační technologie - Bezpečnostní techniky - Soubor postupů pro řízení bezpečnosti informací. Praha: Český normalizační institut 2008.
DOUCEK, P., NOVÁK, L. a SVATÁ, V. Řízení bezpečnosti informací. Praha: Professional Publishing 2008. ISBN 978-80-86946-88-7.
INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 20000-1:2011. Information technology - Service management - Part 1: Service management system requirements. Geneva: International organization for Standardization 2011.

Vedoucí diplomové práce: Ing. Petr Sedlák

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2011/2012.

L.S.

Ing. Jiří Kříž, Ph.D.	doc. RNDr. Anna Putnová, Ph.D., MBA
Ředitel ústavu	Děkan fakulty

V Brně, dne 21.05.2012

Abstrakt

Diplomová práce se zabývá návrhem procesů pro skutečnou společnost poskytující služby v oblasti informačních technologií. Výsledkem práce jsou modely navržených procesů, včetně návrhu potřebného informačního systému a vyhodnocení souladu navržených procesů oproti řadě norem ISO/IEC 27000 a ISO/IEC 20000.

Abstract

The goal of this diploma thesis is to design processes for existing ICT company mainly providing services. This work contains models of the designed processes and proposes convenient information system. All the designed processes are evaluated against ISO/IEC 27000 and ISO/IEC 20000 standards.

Klíčová slova

Návrh procesů, outsourcing IT, ISMS, ITSM, bezpečnost informací, informační systém, ISO/IEC 20000, ISO/IEC 27000.

Keywords

Process design, IT outsourcing, ISMS, ITSM, information security, information system, ISO/IEC 20000, ISO/IEC 27000.

Citace

HALLER, M. *Návrh procesů pro společnost poskytující IT služby s ohledem na ISMS a ITSM.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2012. 77 s. Vedoucí diplomové práce Ing. Petr Sedlák.

Čestné prohlášení

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

V Brně dne 24. května 2012

….....

Poděkování

Rád bych poděkoval svému vedoucímu práce panu inženýru Petru Sedlákovi za vlídné a přátelské vedení mé diplomové práce. Také bych chtěl poděkovat své rodině za věnovanou podporu a pochopení během mého vysokoškolského studia.

Obsah

Úvod

V současné době podnikám v oblasti informačních technologií se zaměřením na služby. Vlastním společnost PATRON-IT s.r.o., která je pokračováním mého podnikání na základě živnostenského oprávnění. Společnost aktuálně nemá stále zaměstnance, ale vzhledem k rostoucímu objemu práce budou již brzo potřeba. Protože si uvědomuji, že pracovní procesy pro jednoho člověka jsou zcela jiné než pracovní procesy pro více lidí, rozhodl jsem se zvolit si diplomovou práci na téma návrhu procesů pro svoji společnost.

V práci musím nejprve identifikovat procesy, na které se zaměřit, a navrhnout vhodnou organizační strukturu společnosti. Identifikované procesy dále definuji a vytvořím jejich model.

Vzhledem k vysoké ceně kvalifikované lidské práce a snaze o vyšší efektivitu procesů je v současné době standardem, že všechny procesy jsou podporovány výpočetní technikou. Při definování procesů se budu snažit využívat výpočetní techniku v co největší míře. Výsledkem tedy nebude pouze definice a model procesu, ale pokusím se navrhnout a připravit vhodný informační systém, který bude navržené procesy podporovat.

Protože výsledek mé práce skutečně aplikuji na svoji společnost, potřebuji, aby navržené procesy byly dostatečně kvalitní. Z toho důvodu porovnám soulad navržených procesů oproti řadě norem ISO/IEC 20000 (management služeb informačních technologií) a ISO/IEC 27000 (systém řízení bezpečnosti informací).

1 Teoretická výhodiska

V této kapitole se věnuji zdrojům, ze kterých jsem vycházel při praktické části práce. Kapitoly s jednotlivými zdroji jsou seřazeny dle významnosti.

1.1 Knihy

Během teoretické přípravy na tuto diplomovou práci, studia a podnikání jsem přečetl k tématu řadu knih. Rád bych jich zde pár zmínil.

Ohledně návrhu a zlepšování procesů mne zaujala kniha „Zlepšování podnikových procesů“[1] od autorky Aleny Svozilové. Kniha je určitým průvodcem v oblasti podnikových procesů a jejich zlepšování. Obsahuje jak teoretické pojednání o jednotlivých metodách, tak i kroky pro jejich úspěšnou aplikaci.

V oblasti prodeje a vylepšování mne zaujala kniha „Dokonalé služby“[2]. Autor Pavel Vosoba v této knize glosuje o chybách a nedostatcích služeb, se kterými se během svého života setkává. Přínosem knihy je autorův bystrý pohled na služby, kdy na ně pohlíží z pohledu zákazníka. Velmi přínosné pro mne byly také články marketingového poradce Pavla Řehulky[1].

Pro oblast bezpečnosti informací je hodnotná kniha „Řízení bezpečnosti informací“[3]. Autoři v knize popisují a porovnávají jednotlivé standardy bezpečnosti informací. Obsahem knihy je také postup a postřehy pro zavádění těchto bezpečnostních standardů.

V případě řízení bezpečnosti informací jsem čerpal z knihy „Softwarové právo“[4]. Kniha se zabývá právem v oblasti IT, je přehledně členěná a srozumitelná. V knize jsou pro mé podnikání užitečné informace, a to v oblasti softwarových licencí, pracovních smluv se zaměstnanci a smluv se zákazníky.

Pro modelování procesů v BPMN byla přínosná dokumentace oficiální „Business Process Model and Notation (BPMN)“[5].

1 Viz domovská stránka http://www.jakzvysitprodej.cz/.

1.2 Předměty

Práce čerpá z řady předmětů magisterského studia. Obzvláště přínosnými byly předměty „Management informační bezpečnosti“, „Systémová integrace“ a „Management počítačových sítí“.

1.3 Vlastní zkušenosti

Při návrhu jsem vycházel i z mé tříleté podnikatelské praxe, bakalářského studia na Fakultě informačních technologií (VUT) a spolupráce s ostatními podnikateli. Vlastní zkušenosti byly cenné zejména při rozhodování nad tím, které metody a software použít.

1.4 Normy

Při zpracování práce jsem využil taktéž norem ISO, jelikož navržené procesy by na ně měly brát ohled. Práce se dotýká norem:

- „ISO/IEC 20000-1:2011 - Information technology - Service management – Part 1: Service management system requirements“,[6],
- „ČSN ISO/IEC 20000-2:2007 - Informační technologie - Management služeb - Část 2: Soubor postupů“[7],
- „ČSN ISO/IEC 27001:2006 - Informační technologie - Bezpečnostní techniky - Systém managementu bezpečnosti informací – Požadavky“[8],
- „ČSN ISO/IEC 27002:2008. Informační technologie - Bezpečnostní techniky - Soubor postupů pro řízení bezpečnosti informací“[9].

2 Profil společnosti

Společnosti PATRON-IT s.r.o. byla založena dne 12.5.2011. Vznikla jako přirozené pokračování mého podnikání na základě živnostenského zákona. Jediným vlastníkem a zároveň i jednatelem společnosti je Martin Haller (já). Společnost sídlí v IBC centru v Brně ve virtuální kanceláři. V současné době nemá žádné zaměstnance na plný úvazek ani kancelářské prostory. Společnost se zabývá poskytováním služeb v oblasti ICT resp. outsourcingem ICT.

Ilustrace 2.1: Logo společnosti PATRON-IT s.r.o. (Zdroj vlastní).

2.1 Vývoj společnosti

V následujících podkapitolách se věnuji vývoji společnosti od prvních podnikatelských kroků, přes současnost až k budoucí vizi. Krátký popis vývoje společnosti považuji v této práci za důležitý pro plné pochopení mých myšlenek a postupů rozebíraných dále.

2.1.1 Historie

Podnikat jsem nezačal s tím, že bych měl podnikatelský záměr a finanční kapitál. Měl jsem pouze čas, znalosti a potřebu vydělat si peníze.

V dubnu roku 2009 jsem si založil živnost a začal oslovovat první zákazníky. V té době jsem hlavně hledal oblast, ve které bych se mohl uchytit. Dělal jsem především správu sítě a tvorbu webových prezentací. Získával jsem první zákazníky a zkušenosti.

V roce 2010 jsem dokončil své bakalářské studium na fakultě informatiky a z důvodu podnikání jsem se rozhodl jít studovat na fakultu podnikatelskou. V tomto roce jsem se stal také plátcem DPH, díky čemuž jsem mohl svým zákazníkům dodávat i hardware.

V roce 2011 jsem se z kvůli snížení rizika ztráty majetku rozhodl založit společnost s ručením omezeným. Dalším důvodem založení společnosti byl můj názor, že v České Republice zákazníci preferují spíše společnosti než živnostníky. V tomto roce jsem pokračoval v získávání nových zákazníků a začal jsem zjišťovat, že na vše již časově nestačím.

2.1.2 Současnost

Současností je aktuální rok 2012, kdy mám již práce více než mohu stihnout, jsem zavalen různými úkoly, od administrativních záležitostí a jednoduchých servisních úkonů až po náročné instalace a implementace serverových instalací.

Na práci již nejsem sám, ale mám několik spolupracovníků (na dohody o provedení práce nebo živnostníky). Jelikož jsem si do současnosti dělal vše sám a vše jsem měl v hlavě, společnost nemá definovány žádné procesy. Veškerá koordinace je neefektivní, společnost je na mé osobě závislá, stejně tak zákazníci, kteří jsou zvyklí na můj „obličej“. Nemohu mít žádnou dovolenou a pracuji od rána do večera.

Společnost získává další zakázky a zákazníky, je ji tedy třeba více profilovat, odříznout vedlejší aktivity a definovat procesy.

2.1.3 Budoucnost

Do budoucna očekávám růst počtu zákazníků a zakázek. Růst by mohl být také podpořen mým větším časovým fondem, díky dokončenému prezenčnímu studiu. Společnost by do dvou let měla mít alespoň dva stále zaměstnance na pozici techniků. Do tří let by měla získat třetího technika a obsadit pozici vedoucího technika.

Potřebuji tedy vytvořit takový systém, který bude schopen provozovat společnost v efektivním chodu i při počtu více techniků. Přičemž moje práce by se měla postupně přesouvat z technických prací na obchod a řízení společnosti.

2.2 Marketing a strategie

abych byl schopen navrhovat firemní procesy, musel jsem si nejprve ujasnit následující věci.

Definovat cílový trh. Například jak velké zákazníky oslovovat, zda volit zákazníky dle lokality.

Stanovit jaké služby má společnost poskytovat. Do této doby jsem poskytoval vše za co byl někdo ochoten zaplatit (samozřejmě v rámci ICT). Došlo mi však, že rozsah poskytovaných služeb je tak rozsáhlý, že již nejsem časově schopen sledovat veškeré trendy a že některé oblasti jsou finančně zajímavější než jiné.

Jak mají být služby poskytovány zákazníkům, na co klást důraz a jaký z toho musí mít zákazník pocit. Po poradě s kolegou, který dělá to samé akorát v jiném městě jsme přišli s určitým konceptem.

2.2.1 Cílový trh

Společnost se zaměřuje pouze na firemní zákazníky z Brna a okolí. Zaměření na firemní zákazníky je z důvodu poskytování vysoce odborných prací, které by u nepodnikatelů nenašly odběratele.

Omezení lokalitou je z toho důvodu, že u námi poskytovaných služeb je někdy potřeba zákazníka fyzicky navštívit.

Průměrný zákazník společnosti má celkem deset osobních počítačů (notebooků a desktopů) a jeden až dva servery. Jedná se o zákazníky, kteří nemají svého interního správce sítě, nebo jejich správce sítě není na některé úkony dostatečně kvalifikován.

Společnost upřednostňuje zákazníky se zájmem o dlouhodobou smluvní spolupráci, než o jednorázový servis. Tomu odpovídá i ceník a rozsah poskytovaných služeb.

2.2.2 Katalog služeb

Naše společnost poskytuje běžné služby jako ostatní ICT firmy. Pro atraktivnější a srozumitelnější prezentování zákazníkům, jsem je však rozdělil do tří balíčků, které popisuji v následujících kapitolách.

Společnost samozřejmě také poskytuje i jednorázové služby jako jsou poradenství, servis zařízení, instalace nového software atd. Avšak preferujeme stálou smluvní spolupráci se zákazníky. Jednorázové služby jsou zákazníky využívány spíše k odzkoušení naší společnosti.

2.2.2.1 Správa sítí

Služba, kdy naše společnost převezme odpovědnost za kompletní správu sítě. Svým zákazníkům poskytujeme následující služby:

- *Servis*: v případě poruchy nebo problémů pomáháme zákazníkům pomocí vzdáleného připojení nebo fyzické návštěvy v provozovně.
- *Implementace nových služeb*: instalujeme a konfigurujeme pro zákazníka nové služby a HW, včetně odborného poradenství.
- *Pravidelné kontroly*: pravidelně kontrolujeme zákazníkovo ICT prostředí, zda je vše v pořádku, nedošlo k narušení viry, pozměnění konfigurace, instalaci nežádoucího softwaru, nebo zda nedochází k selhávání hardwaru. Aplikujeme bezpečnostní aktualizace pro aplikace, operační systém a antiviry.
- *Konzultace*: poskytujeme zákazníkům konzultace vedoucí ke snížení nákladů, zvýšení bezpečnosti a k nasazení nových služeb.
- *Zastupování*: volitelně zastupujeme zákazníky při vyjednávání služeb ICT od třetích stran (nákup IS, připojení k internetu, pronájem serverů atd.).

2.2.2.2 Správa serverů

Jedná se o určitou pod-službu správy sítě, která je nabízena zákazníkům, kteří mají své správce sítě, ale potřebují pomoct se správou serverů. Služba spočívá v:

- *Neustálý dohled*: zákazníkův server je monitorován naším automatizovaným monitorovacím systémem. Neustále je sledována dostupnost serveru a jeho

služeb, vytížení serveru a zdravotní stav. V případě detekce problémů jsou o tom okamžitě informování technici a jsou zahájeny práce na nápravě problému.

- *Pravidelné kontroly*: server je technikem namátkově kontrolován. Technik kontroluje zejména aktualizace, stav zálohování a zabezpečení serveru.
- *Servis*: na přání zákazníka provádíme změny konfigurace nebo instalaci nových služeb.
- *Poradenství*: zákazníkům poskytujeme poradenství zejména k implementaci nových služeb a zabezpečení.

2.2.2.3 Správa IP telefonů a ústředen

Mnoho zákazníků začalo přecházet na IP telefony a zřizovat si své vlastní fyzické nebo virtuální telefonní ústředny. Začali jsme tedy nabízet i služby v oblasti správy IP telefonů a ústředen, tak aby naše služby byly komplexnější.

V rámci této služby nabízíme zákazníkům pomoc se zaváděním, správou a údržbou IP telefonního řešení. Sami však nejsme telefonními operátory.

2.2.3 Prodejní strategie

Po diskuzi s dalšími podnikateli z oboru jsem stanovil body, na které chci, aby společnost kladla důraz.

2.2.3.1 Odbornost

Základním bodem je odpovídající odbornost. Zákazníci očekávají, že s nimi řeší problém osoba, která danému tématu rozumí. Sám jsem již několikrát zažil, jak konkurenční firma poslala k zákazníkovi technika, který byl odborností spíše na úrovni zkušenějšího uživatele. Teprve když tento technik problém nevyřešil, poslali k zákazníkovi někoho více kompetentního. Zákazníci zvyklí na toto jednání potom velice rádi přecházejí k naší firmě.

Nedostatečná odbornost také vede k častějšímu vzniku chyb, menší spokojenosti zákazníka, zhoršení pověsti, vyšším nákladům na službu a její nižší efektivnosti.

2.2.3.2 Osobní přístup

Zákazníci často oceňují osobní přístup, který jsem jim jako živnostník věnoval. Když měli problém, stačilo jim jedno telefonní číslo, na kterém byl vždy ten stejný člověk ochotný jim pomoci. Za výhody osobního přístupu považuji:

- *Rychlost předávání informací*: technik zná celou zákazníkovu síť i historii řešených problémů a není mu potřeba vše vysvětlovat od začátku.
- *Předcházení nedorozuměním*: každý člověk se vyjadřuje trochu jinak, má jiný smysl pro humor, jinak dává najevo nespokojenost, ironii nebo sarkasmus. Tím že je zákazník v kontaktu vždy se stejným technikem, tak se minimalizují nedorozumění vzniklá na základě chyby v komunikaci.
- *Budování vztahu*: zákazník si na svého technika postupně zvyká a časem mezi nimi vzniká důvěra, která přispívá k pevnějšímu vztahu mezi zákazníkem a technikem a samozřejmě nepřímo mezi zákazníkem a společností. Při vhodném právním ošetření pracovních smluv by se mělo i minimalizovat riziko odchodu zákazníka spolu s technikem.

2.2.3.3 Důvěra

Je třeba, aby zákazník společnosti mohl plně důvěřovat. Zákazník většinou nemá nikoho, kdo by mu řekl, zda s ním společnosti nejedná nečestně, je proto plně odkázán na společnost. Toho jsou si často firmy vědomi a občas toho zneužívají (např. vykáží více práce, nebo si dají více jak stoprocentní marži na hardwaru). Někdy se ale stane, že je toto jednání odhaleno a pak vede ke ztrátě veškeré důvěry a zániku spolupráce. Své konkurenci vděčím již za několik takto získaných zákazníků.

2.2.4 Ceník

Na ilustraci 2.2 je znázorněn aktuální ceník společnosti. Při tvorbě ceníku mi šlo hlavně o jeho přehlednost, srozumitelnost, minimum příplatků a poplatků.

Při návrhu ceníku a stanovování cen jsem vycházel ze svých zkušeností a cen srovnatelné konkurence (dle velikosti společnosti a šíře poskytovaných služeb). Stanovené ceny považuji za průměrné.

Díky tomu, že je většina incidentů řešena na dálku, můžeme si dovolit dát dopravu po Brně bezplatně (ve skutečnosti je cena dopravy rozvolněna do hodinových sazeb).

Platný od 1.1.2012	Pro zákazníky bez smlouvy		Pro smluvní zákazníky	
	Běžný servis	**Servis serverů**	**Správa sítě**	**Správa serverů**
Cena	650 Kč/h	890 Kč/h	490 Kč/h	590 Kč/h
Mimo pracovní dobu	+25%	+25%	bez navýšení	bez navýšení
Doprava po Brně	zdarma	zdarma	zdarma	zdarma
Expresní zásah	dle možností	dle možností	✓	✓
Minutová tarifikace	✓	✓	✓	✓
Osobní technik	✗	✗	✓	✓
Prodej HW bez marže	✗	✗	✓	✓
Telefonická podpora	✗	✗	✓	✓
Vzdálená správa	✗	✗	✓	✓

Ilustrace 2.2: Platný ceník společnosti (zdroj vlastní).

3 Návrh procesů

Tato kapitola je stěžejní kapitolou mé diplomové práce. Jejím výsledkem má být návrh procesů pro moji společnost. Těmito procesy se bude v budoucnu společnost řídit, aby naplnila moji vizi budoucnosti z kapitoly 2.1.3 Budoucnost.

Mým cílem není popsat veškeré procesy, které ve firmě mohou být. Chci popsat procesy, jež se ve firmě opakují nejčastěji a u kterých cítím největší možnosti zlepšení. Některé procesy se opakují zřídka a ještě se mi u nich nepodařilo najít podobnost a vzorec, abych je mohl definovat. Proto chci s jejich definováním ještě počkat. Jejich definování by mne stálo hodně času a mohly by se v krátké době výrazně měnit.

Zkráceně řečeno, jde mi o definování procesů, které mně umožní poskytovat služby s rovnoměrnou úrovní kvality, avšak nebude příliš časově náročné a neomezí kreativitu a iniciativu zaměstnanců.

Abych mohl začít navrhovat procesy, považuji za důležité nejprve popsat současný stav procesů ve společnosti.

Dále budu pokračovat požadavky na budoucí procesy. Tyto požadavky budou vycházet z mých zkušeností, nápadů, názorů, nedostatků současných řešení a odborné literatury.

3.1 Současný stav

V současné době začínám mít více práce než dokážu sám zvládnout. Proto jsem začal zaměstnávat brigádníky na dohody o provedení práce a využívat živnostníky. Bohužel společnost nemá žádné definované a dokumentované procesy.

Společnost je v současné době plně závislá na mně a já jsem jejím „nevolníkem“. Je pro mne komplikované odjet na dovolenou, jelikož by se mohl stát nějaký incident a já ho musel začít řešit z důvodu zachování dobré úrovně služeb (a pak také SLA). V současné době není společnosti schopna jakéhokoliv běhu bez mé osoby.

3.1.1 Přidělování práce

Většinu věcí mám v hlavě a vše jde přeze mne. To je velice neefektivní, jelikož všichni zákazníci volají mně, já pak sháním techniky a přiděluji jim práci. Když oni něco nevědí, tak mi zase volají zpátky. Po dokončení práce mi zase volají, aby mi sdělili výsledky a já volám zákazníkům, zda bylo vše v pořádku. Již teď je tento systém velmi neefektivní a časově náročný.

Věc se komplikuje ještě více, když některý technik není zrovna dostupný a je třeba incident řešit okamžitě. V takovém případě se pokouším sehnat někoho jiného, v nejhorším případě musím řešit problém sám.

3.1.2 Fakturace

Jelikož smluvním klientům se fakturuje vždy souhrnně na konci měsíce, poznamenávám si vždy veškeré úkony do textového souboru. Na konci měsíce shrnu a vystavím fakturu. Účetnictví je prováděno externím pracovníkem na softwaru vlastněným společností. K účetnictví se používá program Pohoda[2] ve verzi Profi. Ve stejném programu jsou i vystavovány faktury.

Do nedávné doby bylo toto řešení dostatečné, avšak nyní, když zaměstnávám další osoby, se to komplikuje. Všichni technici si vedou vlastní evidenci odpracované doby, kterou mi na konci měsíce předávají. Já pak vše musím zkontrolovat, sepsat dohromady a vystavit faktury.

K tomu, aby technici nezapomínali na zapisování odpracované doby, jsou motivování tím, že co nezapíšou, nedostanou proplaceno. Tato motivace se bohužel dá aplikovat pouze u techniků placených od úkonu.

3.1.3 Dokumentace

Jak jsem již psal, většinu informací mám v hlavě. To zahrnuje nastavení ICT prostředí u zákazníků, soupis jejich hardwaru a softwaru. Dále se to také týká různých poznatků, doporučení a zkušeností, které jsem posbíral během doby co dělám správu sítě.

2 Domovská stránka http://www.stormware.cz/ .

3.1.4 Sdílení hesel

Dalším problémem, se kterým se potýkám, je zpřístupňování hesel technikům. Pro žádný systém ani aplikaci nepoužívám stejná hesla, mám jich už za tu dobu několik stovek. Jelikož se jedná o dlouhá a komplexní[3] hesla, používám pro jejich správu aplikaci KeePassX[4]. Tato aplikace umožňuje sdílení hesel pouze sdílením celé databáze hesel. To je velice nepraktické, jelikož si nepřeji, aby měl každý technik přístup ke všem heslům.

3.2 Požadavky na řešení

Z nedostatků současného řešení rozebraného v kapitole 3.1 Současný stav a mých představ o optimálním řešení jsem dal dohromady požadavky na navrhované řešení, které jsou probrány v této kapitole.

3.2.1 Efektivnost

Potřebuji, aby navržené řešení mělo co nejmenší časovou režii a bylo co možná nejvíce automatizované. Jde mi o to, abychom zadáváním dat do informačního systému a prací s ním strávili co nejméně času a informační systém nevyžadoval instalaci dalšího softwaru na klientské počítače.

Jelikož všechny firemní telefonní tarify mají v sobě i internetové připojení, bylo by dobré, aby se navržené řešení dalo obsluhovat i přes mobilní telefony založené na operačním systému Android.

3.2.2 Cena

Výsledné řešení nemusí být bezplatné, avšak je třeba, aby se v nejdražším případě pohybovalo v řádu desítek tisíc korun. Přičemž preferuji nejlepší poměr cena/výkon.

3.2.3 Respektování prodejní strategie

Potřebuji, aby řešení respektovalo a podporovalo prodejní strategii stanovenou v kapitole 2.2.3 Prodejní strategie. Jmenovitě aby podporovalo osobní přístup

3 Skládající se z malých a velkých písmen, číslic a speciálních znaků.

4 Domovská stránka http://www.keepassx.org/ .

k zákazníkům. Zvyšovalo důvěru zákazníků ve společnost tím, že zákazníci musí z řešení cítit stabilitu, profesionalitu a zabezpečení jejich dat. Zákazník musí mít vždy pocit, že technik řešící jejich problém ví, co dělá, a zná zákazníkovo ICT prostředí.

3.2.4 Jednoduchost

Řešení by mělo být jednoduché na ovládání. To znamená, že by nemělo obsahovat příliš mnoho nevyužívaných funkcí. Uživatelská rozhraní by měla obsahovat pouze používané prvky (tlačítka, ukazatele atd.).

Jednoduchost by měla být také ve správě řešení, například aktualizace, zálohování, obnovení ze záloh, přesunu na jiný server.

3.2.5 Živý přehled

Je třeba, aby řešení umožnilo odpovědným osobám sledovat co se právě děje. Například aby se dalo sledovat na čem zrovna technici pracují, jaké mají zákazníci problémy, jak se pracuje na jejich nápravě, které problémy byly již vyřešeny, a které čekají již dlouhou dobu na své vyřešení.

3.2.6 Ukládání historie

Výsledné řešení musí zaznamenávat veškeré akce pro pozdější dohledání okolností, audit a reporty. Například když by zákazník reklamoval řešení nějakého incidentu, nebo rozporoval vyfakturovanou částku.

To samé se týká monitorovacího systému, který musí udržovat informace o jednotlivých výpadcích služeb a zařízení, pro tvorbu statistik a reportů.

3.2.7 Sledování odpracovaného času

Pro účely fakturování a sledování efektivity práce potřebuji, aby systém uměl hlídat odpracovaný čas na zakázku, incident, zákazníka a technika. Díky tomu pak budu vědět kolik mám zákazníkovi fakturovat a zároveň budu vědět, kolik mi konkrétní technik vydělal.

Navíc pokud budu mít zaměstnance na plný nebo částečný úvazek, budu vědět kolik za měsíc vydělal a porovnáním nákladů na jeho zaměstnání zjistím, zda je pro

mne výdělečný nebo ztrátový. U zaměstnanců placených od úkonu zase budu vědět kolik toho za měsíc odpracovali a kolik jim mám vyplatit.

3.2.8 Monitorování serverů

Abychom mohli nabízet službu správy serverů viz 2.2.2.2 Správa serverů, potřebujeme, aby systém umožňoval automaticky sledovat servery zákazníků.

Potřebujeme, aby byla pravidelně kontrolována dostupnost serverů, jimi poskytovaných služeb a také jejich vytížení a kondice. V případě problémů, abychom o tom byli co nejdříve informování a mohli začít pracovat na nápravě.

3.2.9 Fakturace

Pro zjednodušení fakturace by bylo dobré, aby systém sám nabídl položky k fakturaci, získané ze systému viz požadavek 3.2.7 Sledování odpracovaného času. Neměl by však automaticky fakturovat vše, ale nechat uživatele vybrat položky k fakturaci. Nakonec by měl vystavit fakturu v současném účetním systému a k tomu připojit přehled fakturovaných úkonů.

Pokud by vše mělo být ideální, měl by také sám tuto fakturu a přehled odeslat na e-mailovou adresu zákazníka.

3.2.10 Databáze znalostí

Řešení musí nabízet možnost dokumentovat nastavení zákazníkova ICT prostředí, včetně inventáře. Dále je třeba, aby se dala vytvářet různá doporučení, jak mají být určité aplikace instalovány, přidělovány IP adresy, konfigurovány firewally atd.

Je třeba aby tyto informace byly dostupné až po přihlášení do systému na základě uživatelských oprávnění.

3.2.11 Sdílení hesel

Potřebuji také vyřešit problém se sdílením hesel. To takovým způsobem aby to bylo co nejvíce bezpečné, jelikož kompromitováním hesel může dojít k nabourání systémů zákazníků a odcizení dat. Což by nejspíše vedlo k soudním sporům, poškození dobrého jména a vysokým finančním ztrátám.

Sdílení hesel musí být umožněno na základě oprávnění, stanovených na skupiny hesel nebo jednotlivá hesla. To takovým způsobem, aby šlo technikům nastavit přístup pouze k heslům, která potřebují pro svoji práci. Například aby technik nemohl přistupovat k heslům zákazníka, který mu nebyl přidělen.

Bylo by také dobré, kdyby byl přístup k jednotlivým heslům monitorován a pořizovány logy. Například abych věděl, že si technik vyžádal zobrazení hesla pro přístup do pošty v určitý den a čas.

3.2.12 SLA[5]

Ve smlouvách uzavíraných se zákazníky se zavazujeme poskytovat služby s garantovanou dobou odezvy, nebo řešení incidentu. Je pro nás proto nutné mít přehled o tom, jak dlouho je již každý incident řešen a být upozorněni, pokud by se zdálo, že incident nebude vyřešen včas.

Pro případné vylepšování a plánování úrovně kvality našich služeb je třeba, aby systém umožňoval tvorbu statistik vztahujících se k rychlosti řešení incidentů a plnění domluvené úrovně služeb.

3.3 Navrhované řešení

Na základě požadavků, které jsem si stanovil v předchozí kapitole 3.2 Požadavky na řešení, jsem navrhl možné řešení, které popisuji v této kapitole.

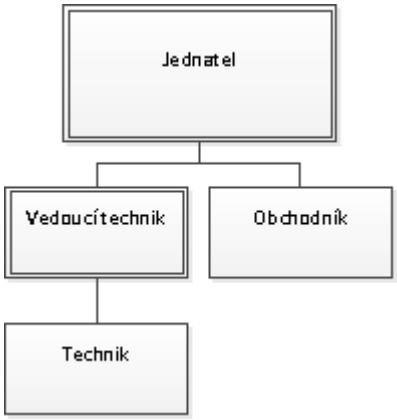
3.3.1 Organizační struktura

Pro navrhované řešení jsem zvolil organizační strukturu vyobrazenou na ilustraci 3.1. Jedná se o role, ne konkrétní osoby. Jedna osoba může mít více rolí, ale většinou bude mít jen jednu. Význam jednotlivých rolí je rozebrán v dalších kapitolách.

Zpočátku bych zastával všechny role já, a všichni zaměstnanci by měli roli techniků. S přibývajícím počtem zaměstnanců bych se nejprve vzdal role technika, následně vedoucího technika a v poslední řadě obchodníka. Dle mého názoru je

5 SLA (Service Level Agreement) je smlouva mezi dodavatelem a odběratelem o úrovni poskytovaných služeb, a to včetně sankcí za nedodržení smluvené úrovně služeb.

organizační struktura optimální pro osm lidí (jednatel, vedoucí technik, obchodník a pět techniků).



Ilustrace 3.1: Návrh organizační struktury (zdroj vlastní)

3.3.2 Přehled procesů

Při sestavování seznamu procesů pro definování jsem vycházel z pohledu poskytovaných služeb. Opět připomínám, že se nejedná o všechny procesy, které ve firmě jsou. Jedná se však o hlavním procesy přímo přinášející příjem společnosti a přidanou hodnotu zákazníkům. Vůbec jsem neřešil procesy pro obchodníka (např. získávání zákazníků, budování vztahů, tvorbu nabídek), a to z toho důvodu, že tuto roli vykonávám já.

Hlavní procesy	Podpůrné procesy
Technik	Obchodník
Servis	Fakturace
Pravidelná kontrola	
Změna v ICT síti	
Monitorovací systém	
Monitorování serveru	

Tabulka 3.1: Seznam procesů, ze kterých se skládá služba „Správa serverů“ (zdroj vlastní).

Jak jsem se již zmínil, při identifikaci procesů jsem vycházel z pohledu poskytovaných služeb (viz 2.2.2 Katalog služeb) mojí společnosti. V tabulce 3.1 jsou

uvedeny procesy pro službu „Správa serverů“ a v tabulce 3.2 zase pro „Správu sítí“. Procesy v tabulkách jsou seskupeny dle role, která proces vykonává.

Hlavní procesy	Podpůrné procesy
Technik	Obchodník
Servis	Fakturace
Pravidelná kontroly	
Změna v ICT síti	
Technik, Hlavní technik, Obchodník	
Dodání HW a SW	
Monitorovací systém	
Monitorování serveru	

Tabulka 3.2: Seznam procesů, ze kterých se skládá služba „Správa sítí“ (zdroj vlastní).

Obě výše jmenované služby spolu sdílí většinu procesů. Proto jsem ještě sepsal všechny procesy do tabulky 3.3 včetně popisu procesů.

Hlavní procesy	
Název	Popis
Servis	Odstraňování závad a problémů v zákazníkově ICT síti, změny v konfiguraci, instalace aplikací. Například instalace nového PC, vytvoření e-mailu nebo odvirování PC.
Pravidelná kontrola	Pravidelné kontrolování zákazníkova ICT prostředí technikem zda je vše v pořádku a nevykazuje odchylky od dokumentovaného stavu. Například kontrola nainstalovaného softwaru, aktualizací nebo zabezpečení.
Změna v ICT síti	Proces provádění větších změn v zákazníkově ICT síti. Například migrace serveru, změna informačního systému, modernizace sítě.
Dodání HW a SW	Proces zajištění dodávky HW a SW na přání zákazníka (od nákupu až po dodání a zprovoznění).
Monitorování serveru	Nepřetržité kontrolování serverů zákazníků, jimi poskytovaných služeb a vytížení. Například zda server není nedostupný.
Podpůrné procesy	
Název	Popis
Fakturace	Proces vystavení faktury, včetně přehledu odvedené práce a odeslání zákazníkovi.

Tabulka 3.3: Soupis všech identifikovaných potřebných procesů (zdroj vlastní).

3.3.3 Externí zdroje informací

Navržené procesy pracují s externími zdroji informací. Těmito zdroji jsou databáze incidentů, znalostní databáze a správa hesel. V této kapitole je každý zdroj popsán dle obsahu a účelu uchovávaných dat. Aplikace, které se o správu těchto dat starají, jsou popsány v kapitole 3.4 Výběr vhodného softwaru.

3.3.3.1 Databáze incidentů

Tento externí zdroj uchovává informace o incidentech. Incidenty jsou například požadavky na podporu, opravy poruch, nové realizace, poptávky po nových službách nebo hardwaru. Incidenty obsahují veškerou komunikaci a práci s nimi související, včetně data, času, místa, obsahu samotné komunikace. Data jsou veřejně nepřístupná.

Data v databázi incidentů jsou určena pro:

- fakturaci,
- výkazy odvedené práce,
- sestavování statistických přehledů (např. výkonost a vytížení zaměstnanců, plnění úrovně služeb, trendy),
- historii pro případné řešení reklamací.

3.3.3.2 Znalostní databáze

Tato databáze slouží zejména pro vedení dokumentace o ICT prostředí zákazníků. V databázi jsou také vedeny pracovní postupy a doporučení. Přístup k databázi je řízen na základě oprávnění. Technici mají přístup pouze k dokumentaci zákazníků o které se starají.

3.3.3.3 Správa hesel

Tento externí zdroj slouží k bezpečnému uchovávání a sdílení všech přístupových údajů, jmen a hesel. Jedná se o přístupy jak k interním firemním systémům, tak i k systémům zákazníků. Tato data jsou neveřejná a přístup je přidělován na úrovni jednotlivých záznamů.

3.3.4 Modely procesů

V této kapitole chci prezentovat modely procesů identifikovaných v kapitole 3.3.2 Přehled procesů. Modely jsou modelovány v BPMN. Každý model je poté detailněji popsán v samostatné podkapitole.

3.3.4.1 Obecný přehled

Než začnu rozebírat jednotlivé procesy, chtěl bych na ilustraci 3.2 ukázat vztahy mezi procesy. Bohužel z nedostatku místa a pro udržení lepší přehlednosti, neobsahuje tato ilustrace procesy „Změna v ICT síti“ a „Dodávka HW a SW“.

Jak je z ilustrace patrné, spouštěčem všech procesů je požadavek od zákazníka („Servis“, a nezobrazené procesy „Změna v ICT síti“ a „Dovávka HW a SW“) nebo uplynutí určitého časového intervalu („Pravidelná kontrola“, „Monitorování server“ a „Fakturace“).

Proces „Servis“ spočívá v nápravě jakýchkoliv problémů ve spolupráci se zákazníkem (oprava je se zákazníkem komunikována a zákazník je informován o všech událostech). Po procesu „Servis“ vždy následuje proces „Fakturace“, který slouží k finančnímu vyrovnání se zákazníkem za poskytnutý servis (služby).

Procesy „Pravidelná kontrola“ a „Monitorování serveru“ jsou pravidelně spouštěny dle definovaných intervalů. Tyto procesy spočívají v kontrole serverů nebo celého ICT prostředí zákazníků. Pokud se během těchto procesů objeví problém, je po jejich ukončení spuštěn proces „Servis“, který zajistí nápravu problému.

Poslední zobrazený proces „Fakturace“ je zahájen buď koncem zúčtovacího období nebo provedením servisu. Jeho výstupem je vystavená faktura, která je zaslána zákazníkovi.

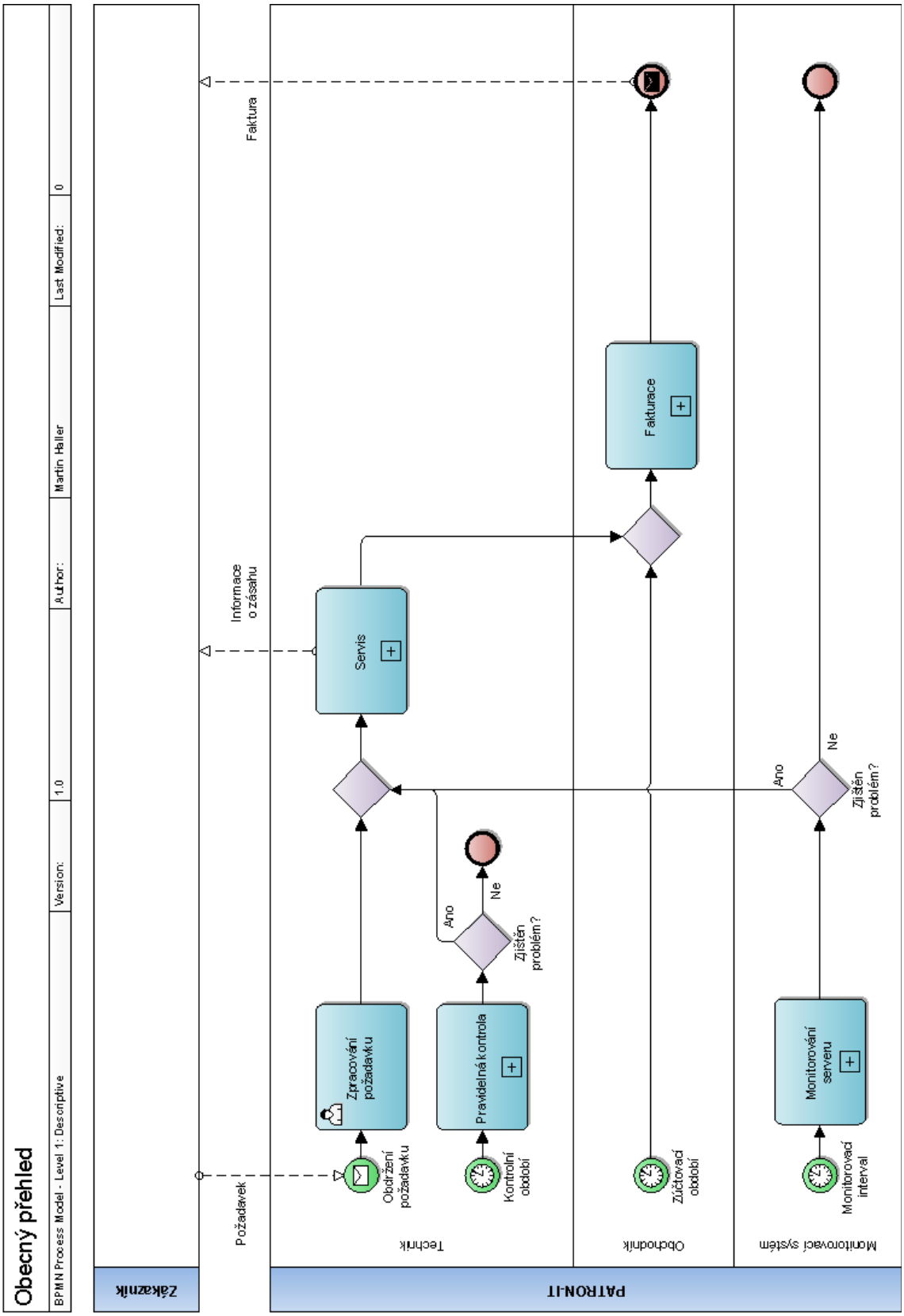
3.3.4.2 Servis

Tento proces, zobrazený na ilustraci 3.3, je pro naši firmu naprosto stěžejní. Slouží k nápravě problémů vzniklých v zákazníkově ICT prostředí, drobným a nesystémovým[6] změnám konfigurace. Tento proces je vykonáván technikem (resp. osobním technikem[7]).

Jak již bylo zmíněno v kapitole 3.3.4.1 Obecný přehled, tento proces je spuštěn na výzvu zákazníka, nebo odhalení problému v jeho ICT prostředí (případně na serveru u služby „Správa serverů“). Na konci tohoto procesu je pak spuštěn proces „Fakturace“.

6 Takové změny, které nemění princip fungování uživatelova ICT prostředí. Jedná se o úkony běžné denní agendy (např. přidání uživatelského účtu, smazání mailové adresy).

7 Technik, který byl organizaci přidělen a primárně se stará o veškeré její technické potřeby.



Ilustrace 3.2: Obecný přehled procesů (zdroj vlastní).

Vstupem procesu je specifický problém (dále jako incident), který má být napraven. Výstupem procesu je odstraněný incident, informování zákazníka o výsledku a podklady pro fakturaci.

Řádné vykonávání procesu může být přerušeno ve dvou případech. Prvním případem je situace, kdy řešení problému trvá příliš dlouho a mohlo by dojít k nedodržení úrovně služeb, za kterých je služba zákazníkovi poskytována (SLA). Druhý případ nastává tehdy, pokud si technik, který incident řeší, neví rady. V obou případech dojde k eskalaci procesu na vedoucího technika. Řešení takovéhoto problému je pak zcela na schopnosti vedoucího technika.

Proces pracuje s celkem třemi externími zdroji informací viz kapitola 3.3.3 Externí zdroje informací.

Samotný průběh procesu je následující. Nejprve jsou o incidentu sesbírány potřebné informace a následně je vše zaznamenáno do databáze incidentů. Do databáze incidentů se uvádí:

- datum a čas vzniku incidentu,
- kým a jak byl incident nahlášen,
- kdo má být o průběhu řešení incidentu informován,
- kdo je zodpovědný za řešení incidentu,
- zjištěné informace o incidentu,
- čas strávený zpracováváním informací o incidentu.

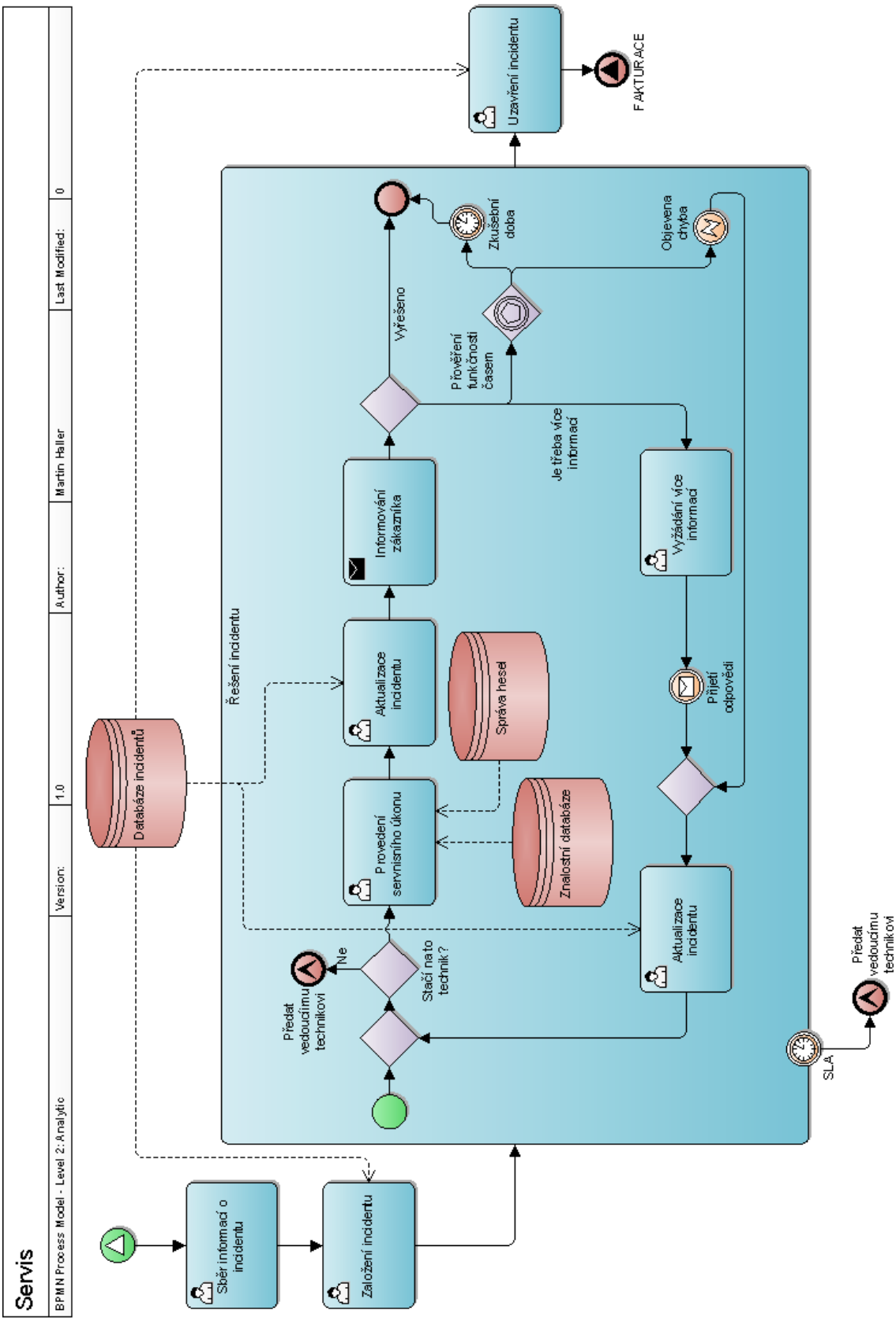
Následně začne probíhat řešení incidentu přiděleným[8] technikem. Na něm je nejprve posoudit složitost a možná řešení incidentu. Pokud zjistí, že sám není schopen provést odstranění incidentu, musí o tom neprodleně informovat vedoucího technika.

Technik provede servisní úkon (např. instalaci, rekonfiguraci, debugování) vedoucí k odstranění incidentu. K dispozici má přitom znalostní databázi, která již může obsahovat správné řešení, postupy nebo doporučení.

O provedeném servisním úkonu je zapsáno stručné hlášení do databáze incidentů s následujícími informacemi:

- datum, čas a místo provedení servisního úkonu,
- odpracovaná doba,

8 Typicky osobní technik daného zákazníka.



Ilustrace 3.3: Model procesu „Servis“ (zdroj vlastní).

- popis servisního úkonu,
- případné změny HW nebo SW.

Osobám, jež mají být o průběhu řešení incidentu informovány (zadány během vytváření incidentu v databázi incidentů), je zaslán e-mail s informacemi o práci na incidentu.

Řešení incidentu může následně probíhat třemi způsoby podle stavu incidentu. Pokud je incident odstraněn (vyřešen), dojde k jeho uzavření v databázi incidentů a proces je ukončen.

Může se stát, že incident je vyřešen, ale pro jistotu je třeba nechat určitou dobu na sledování, zda se incident stále neprojevuje (nevyskytuje). Výběr této možnosti je na uvážení technika řešícího daný incident. Pokud se rozhodne využít této možnosti, vybere určitý časový interval, po který bude incident sledován (např. 1 den, 2 týdny). Pokud se během tohoto intervalu incident neprojeví, je incident uzavřen a proces končí. Pokud se však projeví problémy s pojené s incidentem, je třeba provést řešení incidentu znovu.

Třetí možností je to, že incident nebyl servisním úkonem vyřešen. Technik musí sesbírat více informací o incidentu a pokusit se znovu o jeho nápravu.

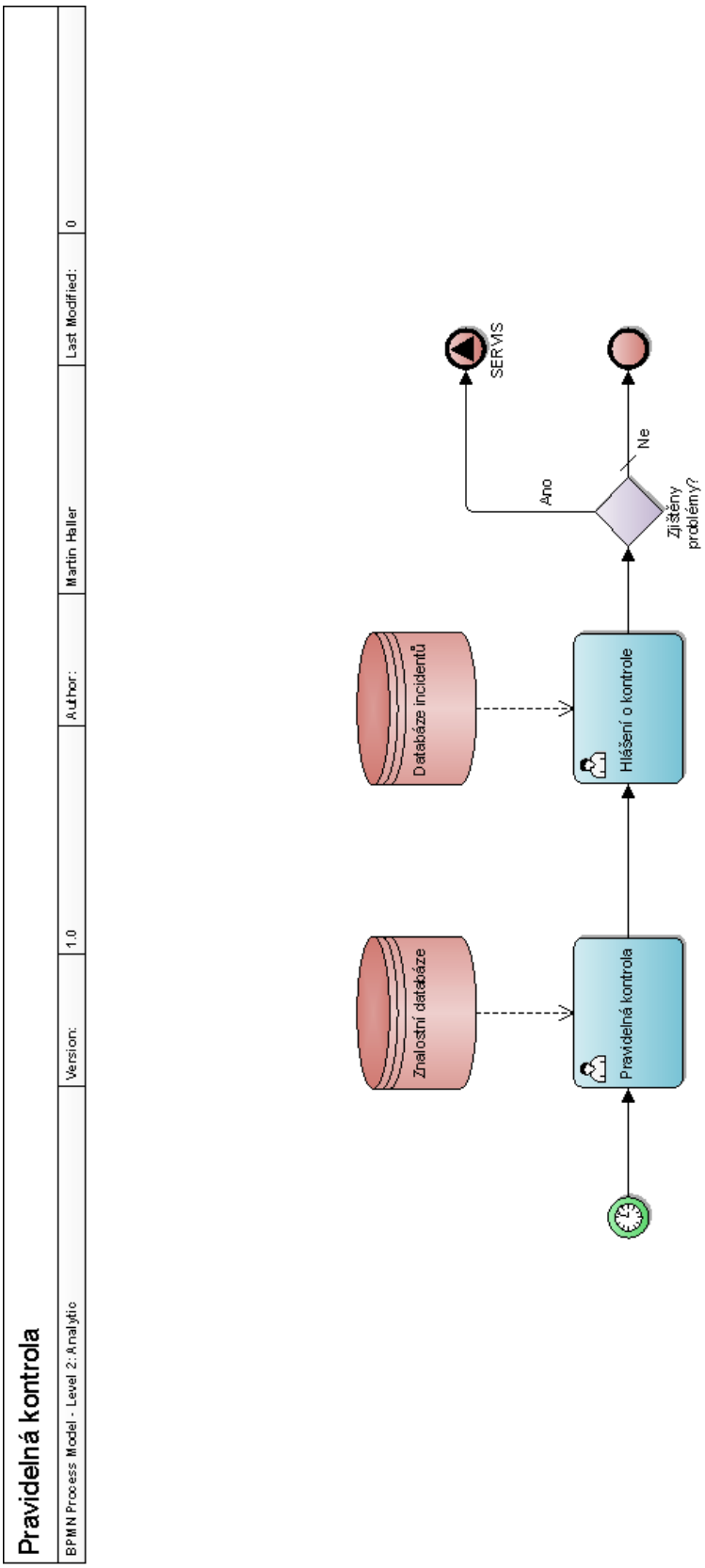
3.3.4.3 Pravidelná kontrola

Model tohoto procesu je zobrazený na ilustraci 3.4. Jedná se o poměrně jednoduchý proces. Proces je prováděný technikem v provozovně zákazníka, a slouží k ověření správného stavu zákazníkova ICT prostředí nebo serveru.

Proces je spouštěn dle přednastaveného časového plánu (např. každý první pátek v měsíci) pro každého zákazníka zvlášť.

Technik provádí kontrolu dle instrukcí, dokumentace zákazníkova ICT prostředí uvedené v databázi znalostí a dle své intuice. Databáze znalostí obsahuje seznam věcí ke kontrole a jakým způsobem mají být kontrolovány. Pokud se technik bude domnívat, že je třeba zkontrolovat i něco navíc, provede kontrolu a podá návrh vedoucímu technikovi na rozšíření databáze znalostí.

Jakmile je kontrola provedena, technik sepíše hlášení o provedené kontrole do databáze incidentů. Do databáze incidentů uvede:



Ilustrace 3.4: Model procesu „Pravidelná kontrola“ (zdroj vlastní).

- datum, čas a místo provádění kontroly,
- odpracovanou dobu,
- případné stručné hlášení (pokud byla nalezena jakákoliv změna oproti dokumentaci zákazníkovy sítě).

Pokud byly během kontroly nalezeny problémy nebo nesrovnalosti (incidenty), které je třeba řešit, je pro každý jednotlivý problém spuštěn proces „Servis“.

Výstupem procesu je hlášení o provedené kontrole a zkontrolované zákazníkovo ICT prostředí.

3.3.4.4 Změna v ICT síti

Tento proces slouží k návrhu a implementaci větších[9] změn v zákazníkově ICT prostředí na žádost zákazníka. Model procesu je zobrazen na ilustraci 3.5.

Proces využívá dvou externích zdrojů dat, a to znalostní databáze a databáze incidentů. Proces je spouštěn na základě žádosti zákazníka o provedení změny v jeho ICT prostředí.

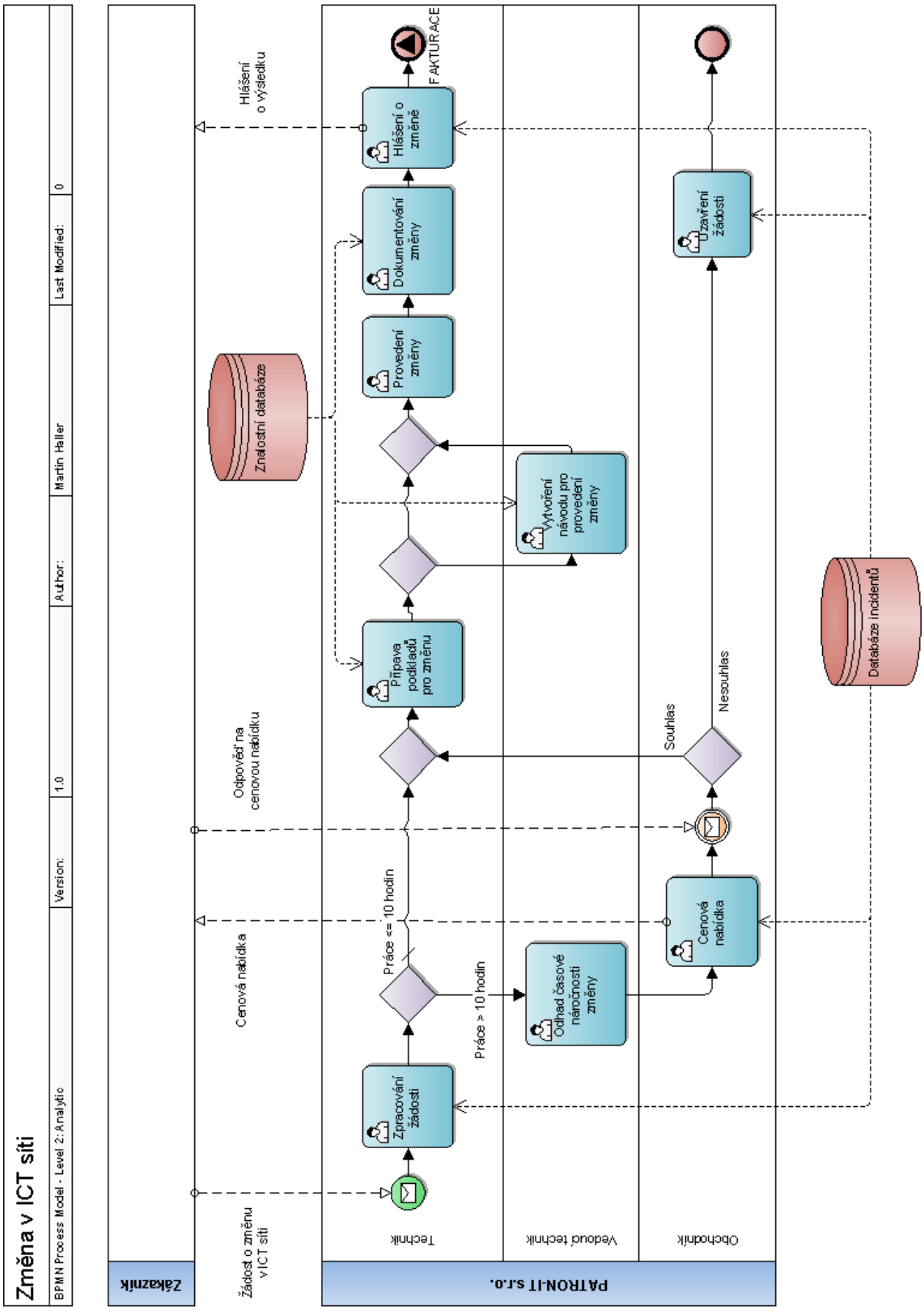
Vstupem procesu je zákazníkova žádost o změnu svého ICT prostředí a výstupem procesu je stav zákazníkova ICT prostředí po žádané změně.

Jak jsem již psal, proces je spuštěn na žádost zákazníka. Tato žádost je přijata technikem, který provede prvotní zvážení žádosti (zda není žádost nesmyslná, neúplná nebo chybná) a zaznamená ji do databáze incidentů.

Pokud technik usoudí, že se jedná o časově nenáročnou žádost (cca do 10 hodin práce), je žádost o změnu schválena a může změnu začít vykonávat. Je-li změna časově náročná, předá ji vedoucímu technikovi, který provede časovou kalkulaci. Časová kalkulace je předána obchodníkovi, který pro zákazníka vytvoří cenovou nabídku, kterou mu pošle. Zamítne-li zákazník cenovou nabídku, je incident uzavřen a nejsou provedeny žádné změny. Souhlasí-li však zákazník s cenovou nabídkou, pokračuje se v procesu dále.

Jakmile je žádost o změnu schválena, připraví si technik podklady pro provedení změny. Podklady je myšlen postup, jak bude danou změnu realizovat. Tyto podklady sestavuje ve spolupráci s databází znalostí.

9 Netriviální změny, které mění způsob fungování zákazníkova ICT prostředí nebo vyžadují plánování provedení změny.



Ilustrace 3.5: Model procesu „Změna v ICT síti“ (zdroj vlastní).

Nenajde-li technik v databázi znalostí podklady, nebo neví jak má změnu realizovat, musí se obrátit na vedoucího technika. Vedoucí technik tyto podklady připraví a zároveň vše zaznamená do databáze znalostí, tak aby v budoucnu mohl tyto podklady připravit sám technik.

Jakmile má technik připravené podklady pro realizaci změny, změnu realizuje. Vzhledem k velikosti a povaze změny provede případně technik úpravu dokumentace zákazníkova ICT prostředí v databázi znalostí.

Na závěr technik provede hlášení o změně do databáze incidentů, kam zapíše podrobnosti o změně, které by mohly být v budoucnu důležité (např. čas, změny v HW a SW, úpravy zabezpečení) a čas strávený realizací změny. Toto hlášení je také zasláno zákazníkovi.

Proces na svém konci spouští proces „Fakturace“, kde dojde k finančnímu vyrovnání se zákazníkem.

3.3.4.5 Dodání HW a SW

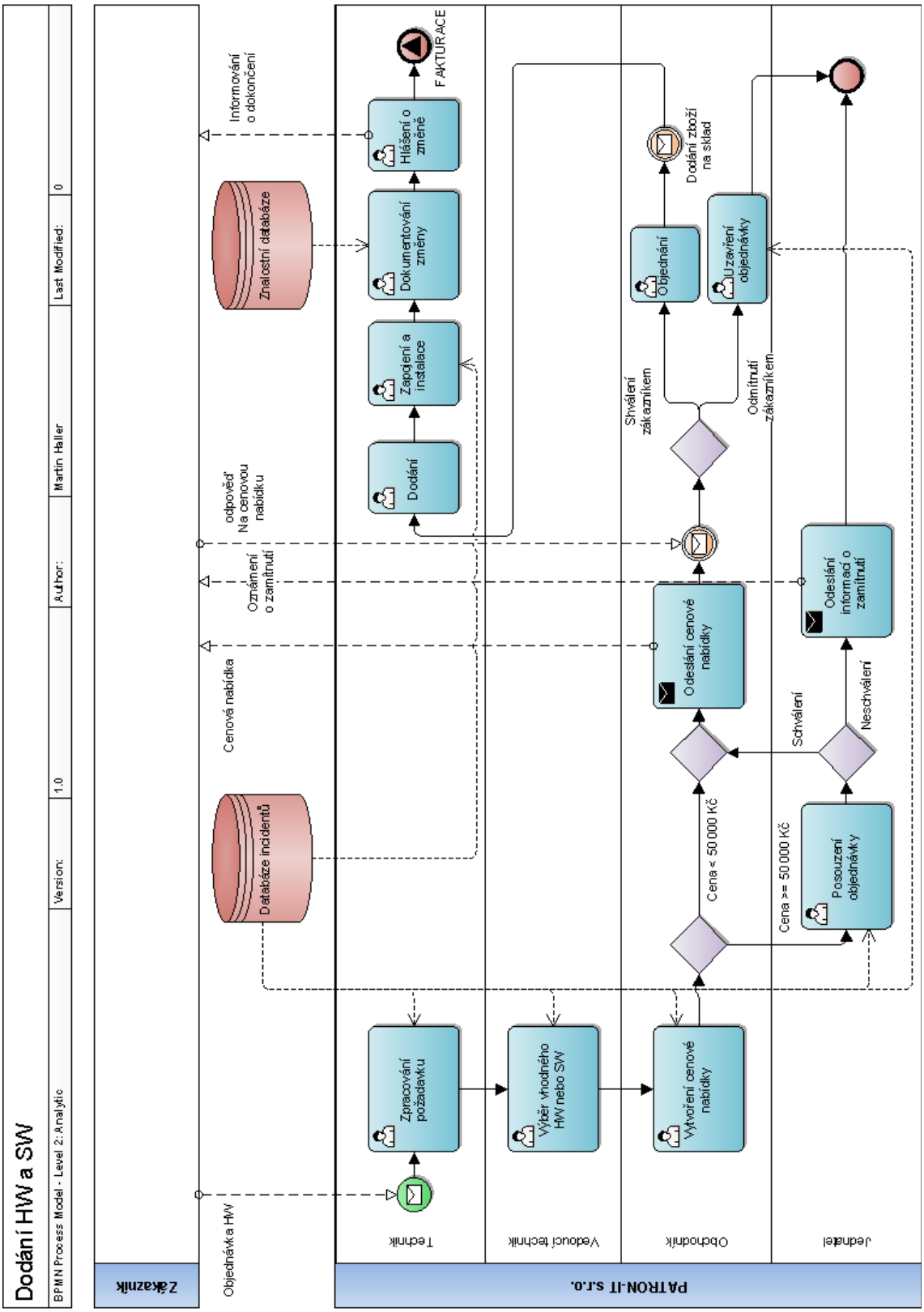
Tento proces se zabývá prodejem hardwaru a softwaru zákazníkům na jejich žádost. Model procesu je zobrazen na ilustraci 3.6.

Proces je tedy zahájen žádostí (potřebou) zákazníka na nový hardware nebo software (dále jen jako „zboží“). Vstupem do procesu je ona zákazníkova žádost a výstupem procesu je dodané a nainstalované zboží.

Zákazník kontaktuje osobního technika s žádostí o nové zboží. Technik žádost zpracuje, případně ji se zákazníkem upřesní a zapíše do databáze incidentů. Následně je vše předáno vedoucímu technikovi, který vybere konkrétní zboží a zapíše do databáze incidentů.

Jakmile je vybráno konkrétní zboží, zpracuje obchodník cenovou nabídku. Pokud je cena vyšší než 50 000 Kč bez DPH, musí vše ještě schválit jednatel, protože se zákazníkům dodává zpravidla na fakturu. Jednatel může nabídku schválit, nebo odmítnout, případně jinak změnit dispozici nabídky (např. vyžadovat platbu zálohou). Cenová nabídka i rozhodnutí jednatele jsou zapsány do databáze incidentů.

Pokud jednatel objednávku neschválí, informuje zákazníka o zamítnutí objednávky včetně důvodu, proč k tomu došlo.



Ilustrace 3.6: Model procesu „Nákup HW a SW“ (zdroj vlastní).

Je-li objednávka schválena jednatelem, je cenová nabídka odeslána zákazníkovi. Ten ji může odmítnout, v takovém případe je objednávka uzavřena a proce končí. Je-li objednávka zákazníkem schválena, obchodník provede objednání zboží.

Jakmile je zboží dodáno na náš sklad, doručí jej osobní technik zákazníkovi, kde provede instalaci a zprovoznění dodaného zboží. Vše je nakonec zaznamenáno v databázi incidentů, včetně odpracované doby.

Nové zboží je také zadokumentováno v dokumentaci zákazníkova ICT prostředí v databázi znalostí.

Na tento proces následně navazuje proces fakturace, kde dojde k finančnímu vyrovnání se zákazníkem.

3.3.4.6 Monitorování serveru

Tento proces je plně automatizován pomocí softwaru ICINGA probíraného v pozdějších kapitolách. Model tohoto procesu (viz ilustrace 3.7) jsem zahrnul pro úplnost a lepší pochopení pro ty, kteří s automatizovanými monitorovacími systémy nemají žádné zkušenosti.

Proces je spouštěn zvlášť pro každý server (ve skutečnosti pro každou sledovanou službu) dle zvoleného monitorovacího intervalu. Systém provede vyhodnocení stavu serveru a služby dle konfigurovaných pluginů a skončí (samozřejmostí je i interní logování událostí).

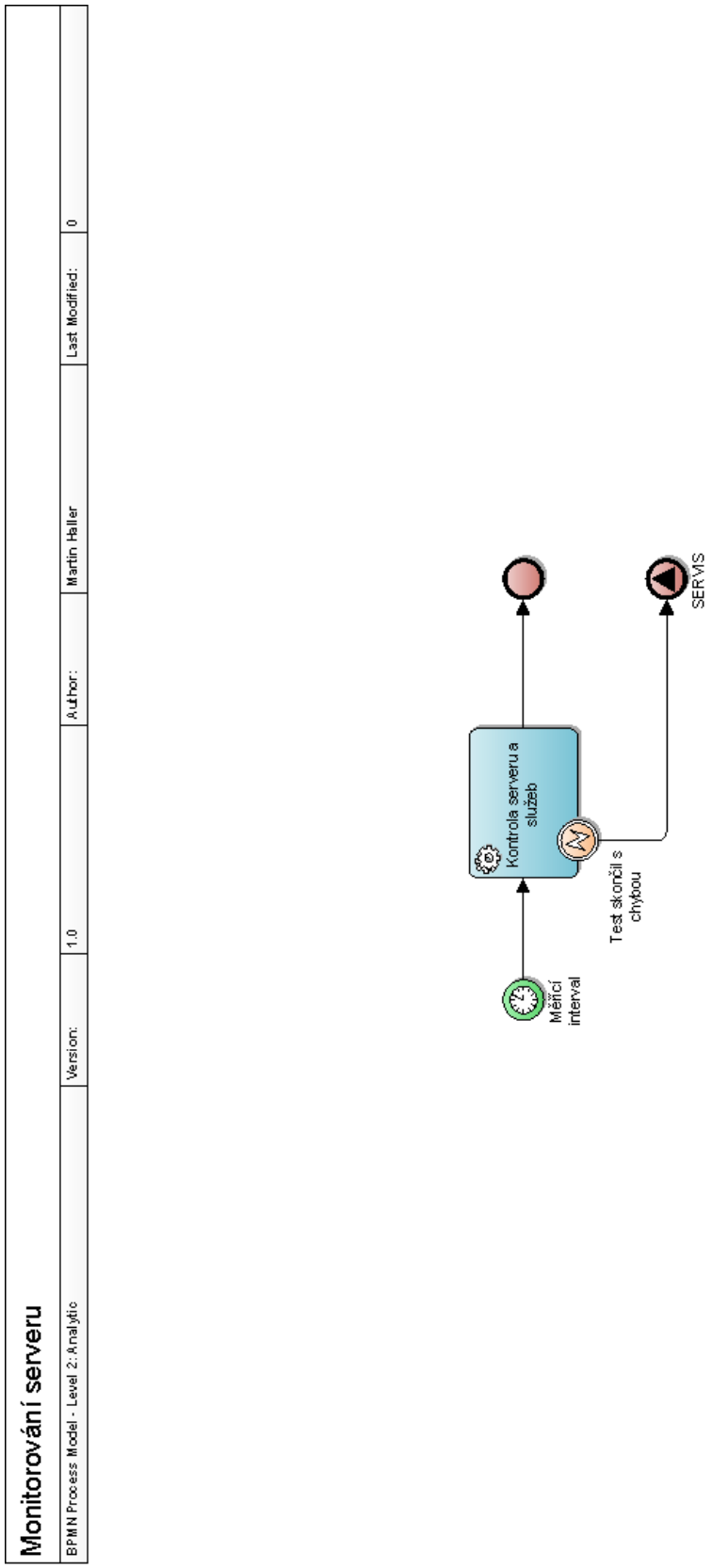
V případě, že test nějaké služby nebo serveru s končí s chybou, dojde k vyvolání procesu servis, kde bude chyba odstraněna.

3.3.4.7 Fakturace

Jedná se o jednoduchý avšak důležitý proces. Model procesu je vyobrazen na ilustraci 3.8. Proces může být vyvolán dvěma způsoby, a to skončením zúčtovacího období nebo zavoláním tohoto procesu.

Výstupem procesu jsou faktura a výkaz odvedené práce, které jsou elektronicky zaslány zákazníkovi.

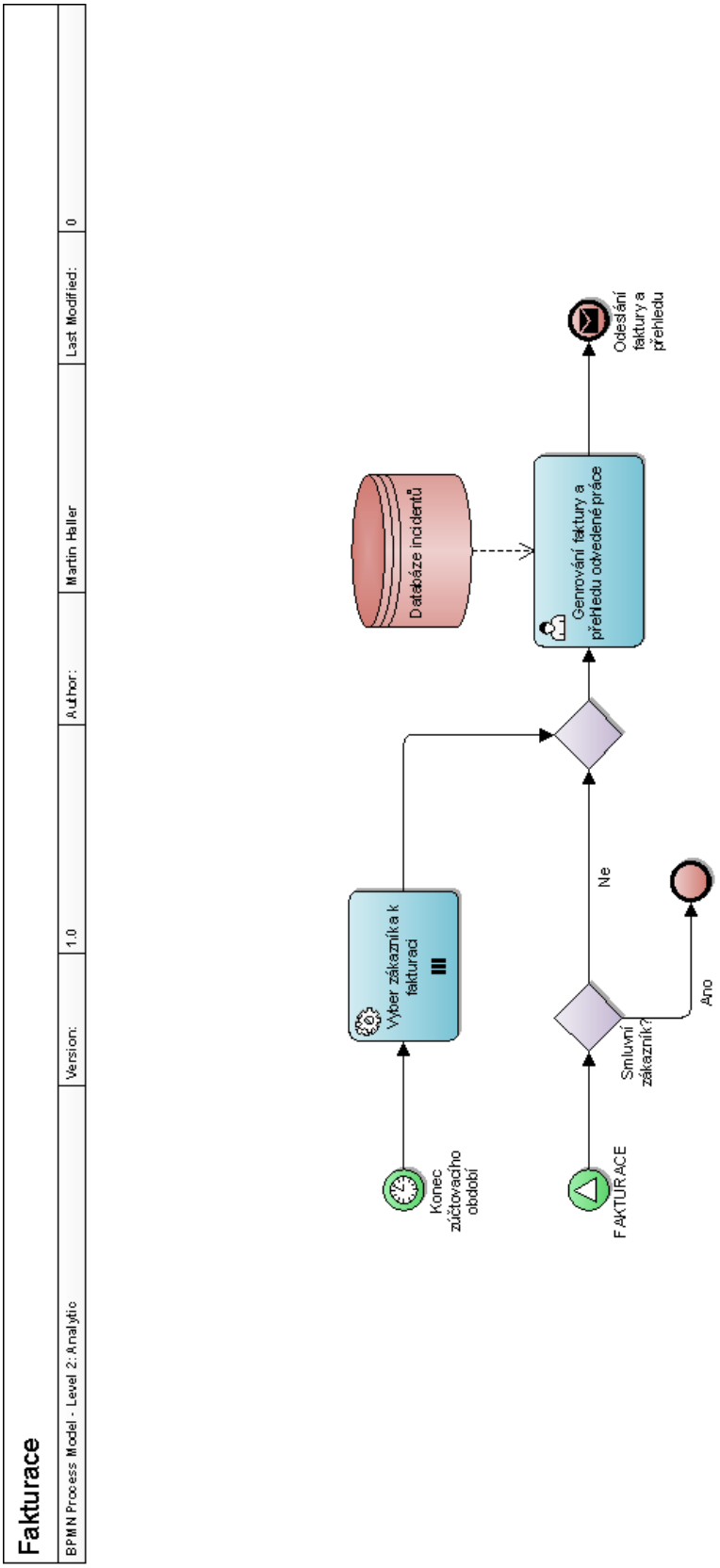
Pokud je proces zavolán jiným procesem, rozhoduje se nejprve, zda zákazník kterému se má fakturovat je smluvním zákazníkem nebo ne. Smluvní zákazníci mají totiž pevně stanovenu souhrnnou fakturaci na konci zúčtovacího období.



Ilustrace 3.7: Model procesu „Monitorování serveru“ (zdroj vlastní).

Proces je vysoce automatizován informačním systémem. Uživatel musí pouze zkontrolovat položky k fakturaci, případně je upravit nebo odložit.

Následně informační systém provede vystavení elektronicky podepsané faktury v účetním systému Pohoda ve formátu PDF. Je také vytvořen přehled fakturovaných položek, také ve formátu PDF. Tyto dva dokumenty jsou archivovány na pevný disk a následně odeslány e-mailovou zprávou zákazníkovi.



Ilustrace 3.8: Model procesu Fakturace (zdroj vlastní).

3.4 Výběr vhodného softwaru

V této kapitole popisuji software, který jsem pečlivě vybral pro realizaci procesů navržených v předchozí kapitole. Výběr softwaru ve skutečnosti neprobíhal tak, že bych nejprve navrhl procesy a pak hledal potřebný software. Návrh procesů šel ruku v ruce s výběrem vhodného a dostupného softwaru.

3.4.1 OTRS Help Desk[10]

Jedná se o systém pro sledování a spravu incidentů (tzv. „help desk system“ nebo „ticket request system“). Je vyvíjen stejnojmennou skupinou společností OTRS, které mají různé právní formy po světě[11]. Software je distribuován jako open source pod licencí „AFFERO GNU General Public License“ verze 3. Systém je v základní verzi bezplatný. Placené jsou pouze některé rozšiřující moduly a podpora.

Jak jsem již psal, hlavní funkcí systému je sledování a správa incidentů. Systém umožňuje automatické a ruční zadávání incidentů do systému. Automatické zadávání probíhá přes stahování e-mailů z nastavených e-mailových schránek (POP3 a IMAP). Přes bezplatné rozšíření je také možné automatické vytváření e-mailů z monitorovacího systému NAGIOS[12] a jemu kompatibilních řešení.

Systém je velice rozsáhlý a nabízí řadu funkcí, pro jejich úplný seznam doporučuji navštívit domovskou stránku. Já bych níže vyjmenoval pouze funkce užitečné pro navržené procesy:

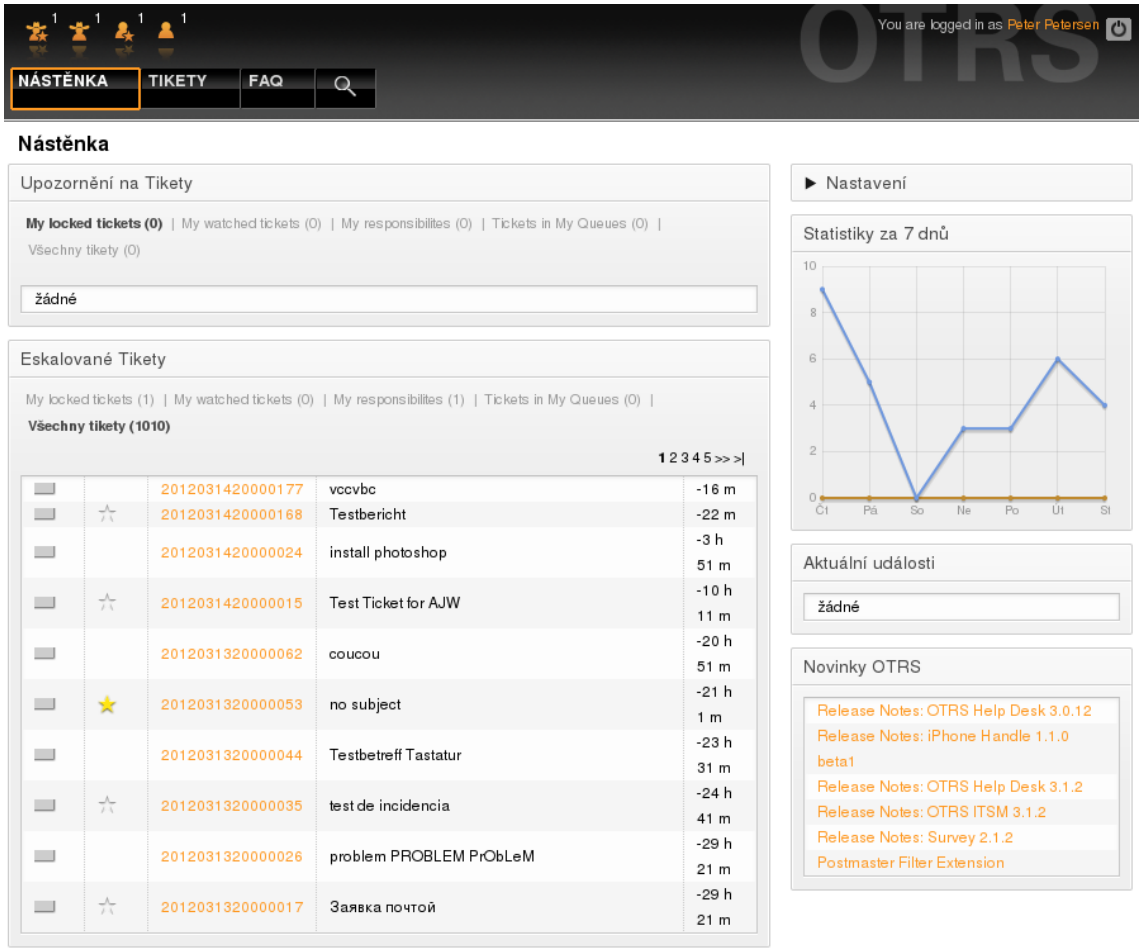
- třídění incidentů dle zákazníka,
- automatické přidělení technika k incidentu na základě pravidel,
- webový přístup pro zákazníky, který jim umožňuje sledovat aktuální stav a historii hlášených incidentů,
- sledování odpracované doby na incidentu,
- automatickou eskalaci incidentů na základě pravidel,
- možnost vytváření šablon pro jednotlivé druhy incidentů,
- automatické odesílání informačních e-mailů o průběhu incidentu,
- automatické sledování plnění SLA (service level agreement).

10 Domovská stránka http://www.otrs.com/en/products/otrs-help-desk/ .

11 Seznam společností je k nalezení na http://www.otrs.com/en/company/locations/ .

12 Domovská stránka http://www.nagios.org/.

Obecně velkým přínosem těchto systémů pro sledování a správu tiketů je možnost managementu sledovat a organizovat práci jednotlivých techniků. Jelikož incidenty zůstávají v systému i po vyřešení, je možné kdykoliv řešit případné reklamace zákazníků na provedený servis.



Ilustrace 3.9: Webové rozhraní systému OTRS Help Desk (zdroj vlastní).

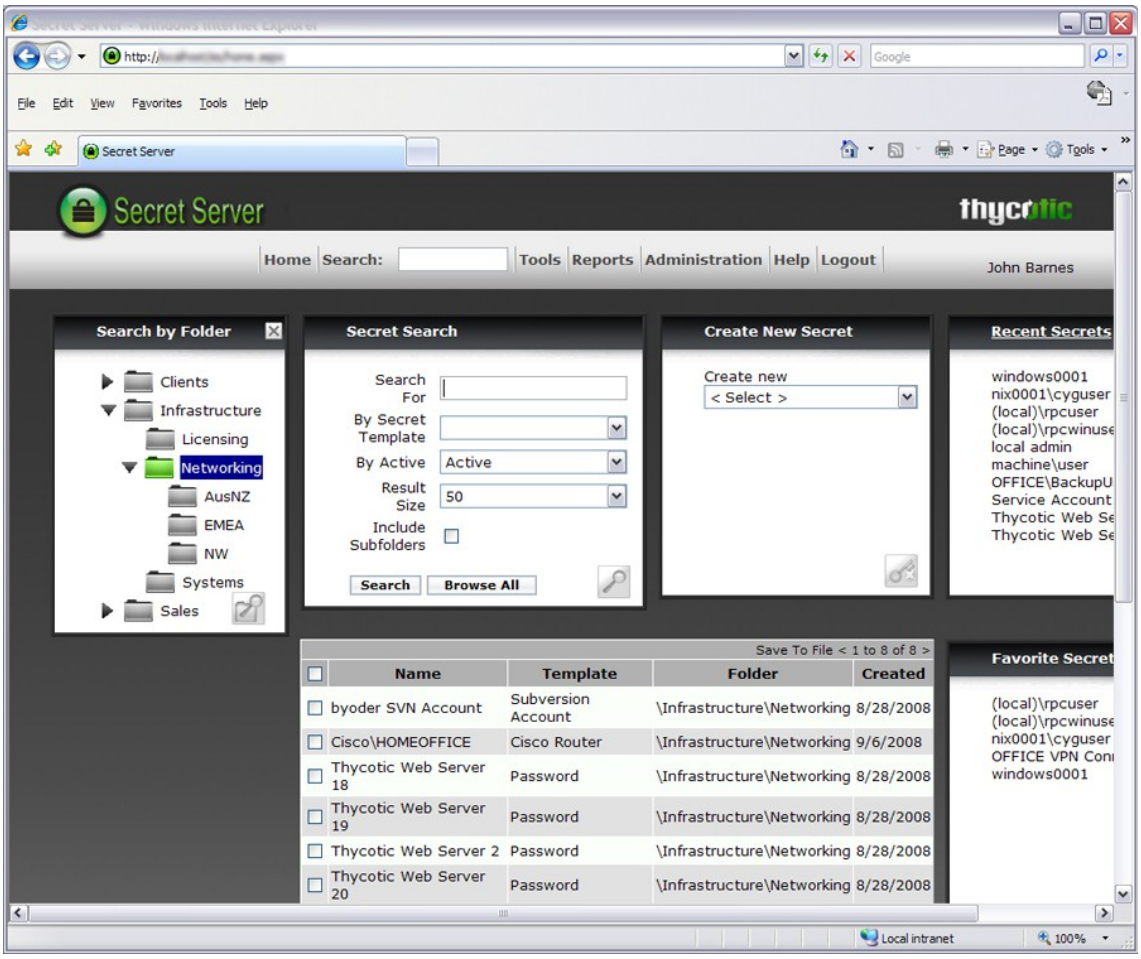
Hlavním uživatelským rozhraním je webové rozhraní (viz ilustrace 3.9) dostupné přes jakýkoliv moderní webový prohlížeč. K systému je také možné přistupovat z mobilních telefonů, a to přes webové rozhraní nebo speciální aplikace.

3.4.2 Secret Server[13]

Jedná se o systém pro bezpečné sdílení hesel mezi uživateli. Systém je vyvíjen společností Thycotic Software Ltd. Systém je nabízen dvěma způsoby, a to jako licence

13 Domovská stránka http://www.thycotic.com/products_secretserver_overview.html .

pro běh na vlastním serveru, nebo jako služba, kdy je systém provozován na serveru poskytovatele, ten se stará o aktualizace a správný běh. Dále existuje několik edic systému dle úrovně funkčnosti (pro potřeby společnosti stačí základní verze standard).



Ilustrace 3.10: Uživatelské rozhraní systému Secret Server (zdroj http://www.thycotic.com/).

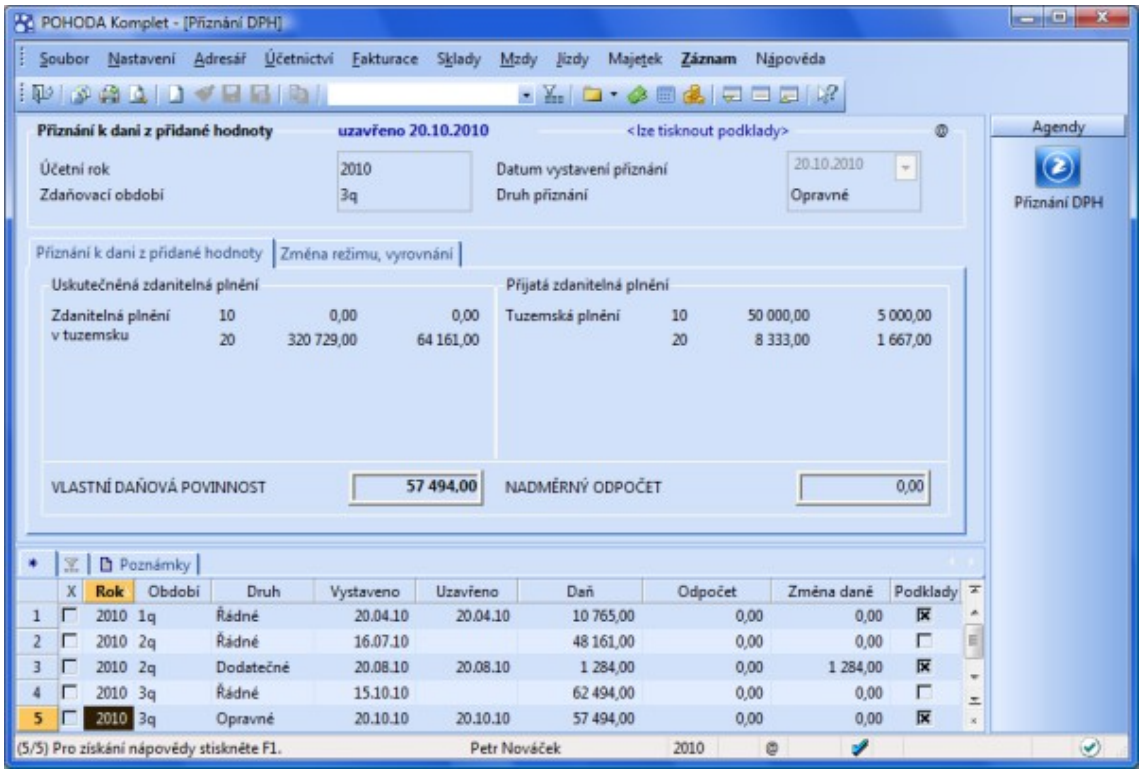
Systém bezpečně uchovává uživatelská jména, hesla, licenční údaje a další důvěrné informace. Správce systému může omezovat přístup k těmto informacím na základě oprávnění. Dokonce je možné, aby uživatel systému využil heslo, aniž by mu bylo zobrazeno (pomocí pluginů). Systém je i schopen sám měnit hesla k podporovaným službám, například SSH, Microsoft Windows, Microsoft SQL serveru.

Mezi další funkce systému patři zaznamenávání přístupu k jednotlivým heslům, integrace s Active Directory. Systém je dostupný přes webové rozhraní (viz ilustrace 3.10) pomocí webového prohlížeče a zároveň pomocí aplikací pro mobilní telefony.

Pro společnost je nejdůležitější hlavně možnost sdílet bezpečně hesla na základě uživatelských oprávnění (tzn. aby měl technik přístup pouze k heslům, které potřebuje).

3.4.3 Pohoda[14]

Pohoda je česká účetní aplikace vyvíjená společností STORMWARE s.r.o. Jedná se o placenou aplikaci, kde se platí za licenci a podporu s aktualizacemi. V současné době již společnost vlastní licenci na verzi Pohoda Profi s podporou a aktualizacemi pro rok 2012.



Ilustrace 3.11: Uživatelské rozhraní aplikace Pohoda (zdroj http://www.stormware.cz).

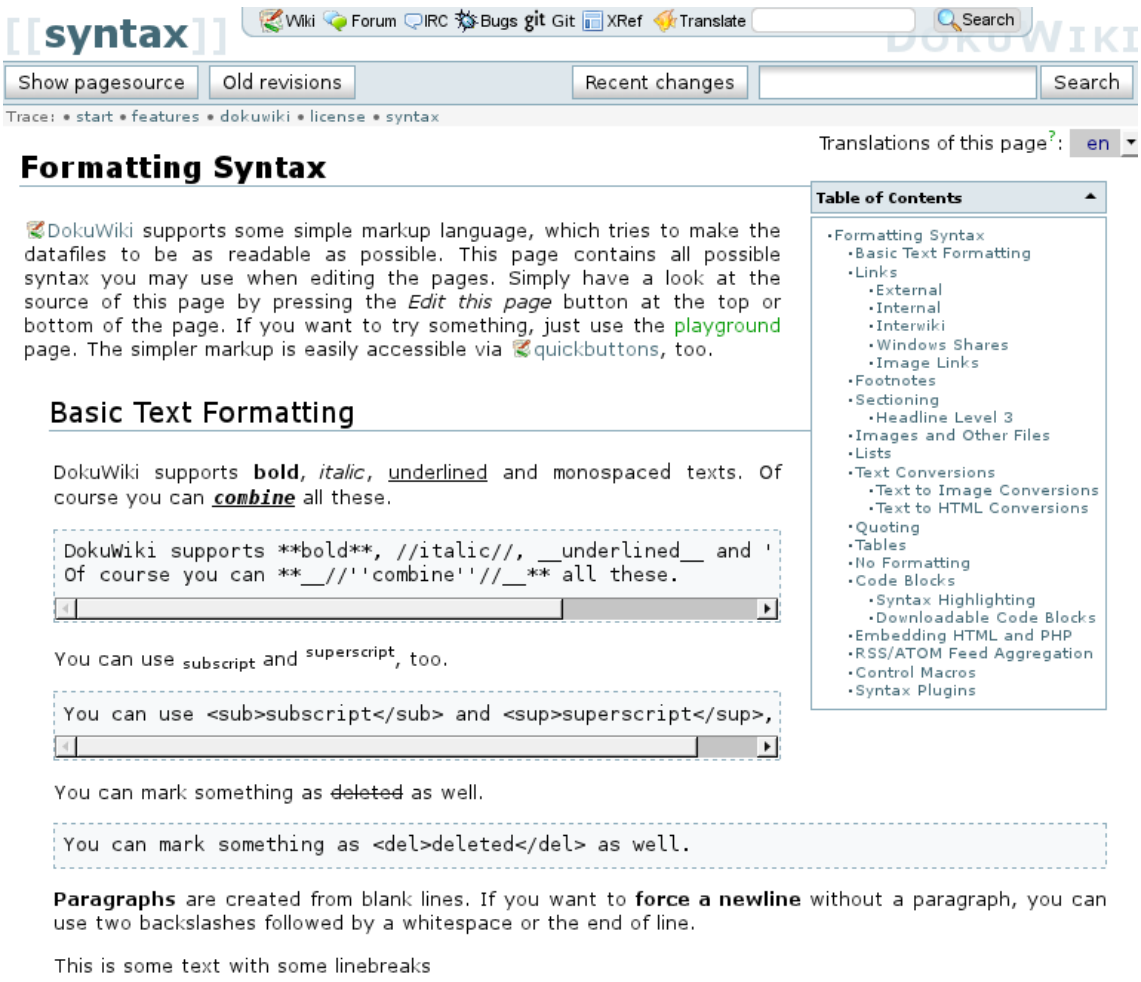
Společnost aplikaci využívá pro fakturaci zákazníkům a vedení účetnictví dle zákona o účetnictví. Aplikace běží jako desktopová aplikace s běžným GUI rozhraním

14 Domovská stránka http://www.stormware.cz/pohoda/ .

(viz ilustrace 3.11) na operačních systémech rodiny Microsoft Windows (verze XP a novější).

3.4.4 DokuWiki[15]

Jedná se o aplikaci pro tvorbu a sdílení obsahu formou webových stránek. Jak je již z názvu patrné, jedná se o aplikaci podobnou té, na které běží světová encyklopedie Wikipedia[16]. Aplikaci vyvíjí pan Andreas Gohr a komunita dobrovolníků vytvořená kolem této aplikace. Jedná se opět o open source aplikaci vyvíjenou pod licencí GNU



Ilustrace 3.12: Uživatelské rozhraní aplikace DokuWiki (zdroj http://www.dokuwiki.org).

15 Domovská stránka http://www.dokuwiki.org/dokuwiki .

16 Domovská stránka http://www.wikipedia.org/ .

General Public License verze 2[17]. Aplikace je dostupná bezplatně pro osobní i komerční využití. Pro přístup k aplikaci se používá webové rozhraní (viz ilustrace 3.12).

Aplikace se dá využívat k dokumentování nastavení ICT prostředí jednotlivých zákazníků a k tvorbě interních doporučení (například jak rozdělovat IP rozsahy, jak nastavovat konkrétní aplikace, jaké používat postupy k preventivním prohlídkám).

Přístup k veškerému obsahu aplikace lze regulovat pomocí uživatelských účtů a oprávnění.

3.4.5 Icinga[18]

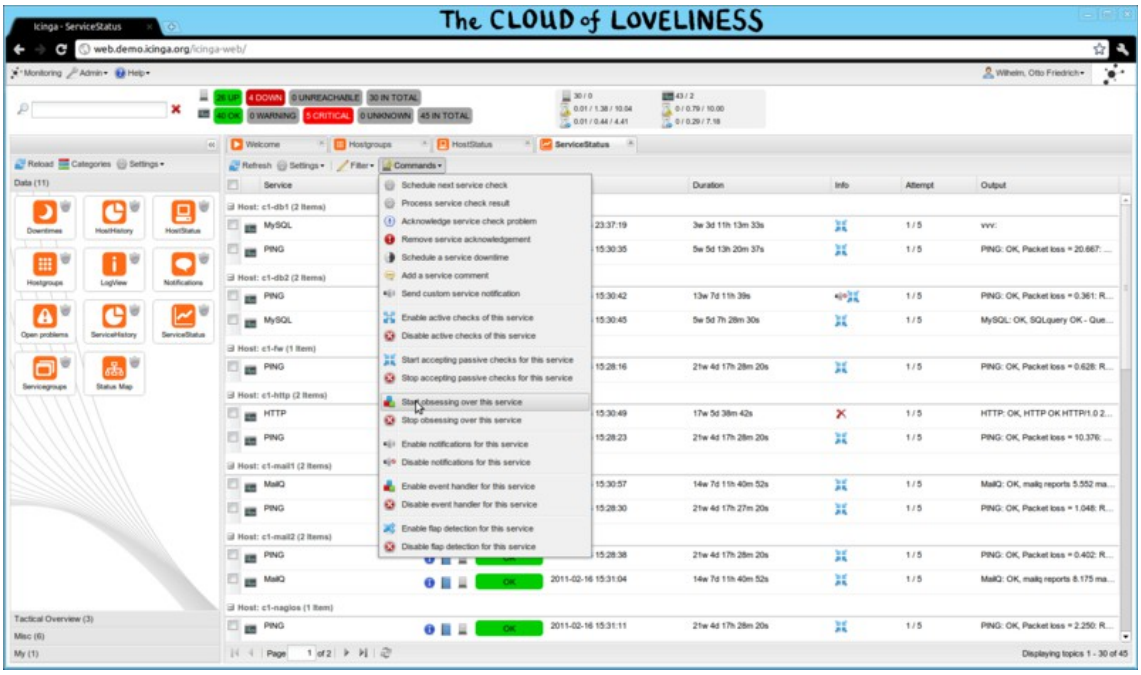
Jedná se o systém pro monitorování zařízení, jimi poskytovaných služeb a využití prostředků. Systém je vyvíjen komunitou pod stejnou licencí jako aplikace DokuWiki (tzn. GNU General Public License verze 2) a vznikl jako „fork“ známějšího monitorovacího systému NAGIOS[19]. Systém je distribuován jako open source pro bezplatné osobní i komerční využití. Uživatelské rozhraní systému je dostupné jako webová stránka přes webový prohlížeč (viz ilustrace 3.13), pro mobilní zařízení je k dispozici speciální verze webových stránek, optimalizovaná na menší displeje telefonů. Existují také aplikace pro mobilní zařízení, které formou widgetu umožňují sledovat aktuální stav monitorovaných zařízení.

Mám-li stručně a technicky popsat činnost systému: systém v stanovených časových intervalech provádí spouštění testů a vyhodnocení jejich výsledků, v případě nežádoucích výsledků, pak může provádět proaktivní[20] opatření nebo nastavenými cestami informovat o nežádoucích výsledcích.

Systém může pravidelně (např. každých pět minut) kontrolovat stav serverů svých zákazníků. Kontrolovat zda je dostupný, běží na něm potřebné aplikace, není přetížen a stav hardwaru je v pořádku (např. disk, teplota, větráky, operační paměť). Systém je schopný sledovat téměř cokoliv. Již v základní distribuci je mnoho modulů[21] a další se dají stáhnout z internetu nebo jednoduše naprogramovat (či naskriptovat).

17 Znění licence na http://www.gnu.org/licenses/gpl-2.0.html .
18 Domovská stránka https://www.icinga.org/ .
19 Domovská stránka http://www.nagios.org/ .
20 Systém může například spustit jiný proces, restartovat cílové zařízení nebo rekonfigurovat aplikaci.
21 Modul, někdy označovaný jako doplněk nebo také anglicky jako plug-in.

Pokud systém zjistí nějaký problém (např. nedostupnost služby, docházející místo na disku), informuje (např. e-mailem nebo SMS) technika zodpovědného za daný server. Pokud technik do určité doby nepotvrdí že začal pracovat na nápravě, jsou o tom problému informováni zbývající technici.



Ilustrace 3.13: Uživatelské rozhraní systému Icinga (zdroj https://www.icinga.org).

3.4.6 Vlastní aplikace

Jelikož aplikace OTRS nemá možnost propojení s účetním systémem Pohoda, bude třeba si toto propojení naprogramovat. Data o odpracované době v aplikaci OTRS jsou dostupná v databázovém úložišti a účetní systém Pohoda má rozhraní pro XML komunikaci, mělo by to být proveditelné.

Aplikace bude pracovat následovně:

- stažení dat ze systému OTRS,
- odfiltrování již fakturovaných položek,
- uživateli se zobrazí položky k fakturaci filtrované podle zákazníka,
- uživatel vybere položky k fakturaci a svoji volbu potvrdí,
- aplikace vygeneruje přehled fakturovaných položek a vystaví fakturu v systému Pohoda,

- faktura i přehled budou odeslány zákazníkovi přes e-mail a zároveň budou archivovány,
- fakturované položky budou v systému označeny jako fakturované.

Tuto aplikaci si vytvoříme svépomocí. Nejspíše ve skriptovacím jazyce PHP s využitím nějakého frameworku (nejspíše Symfony). Aplikace bude dostupná jako webová stránka přes webový prohlížeč a data bude ukládat do databáze a na pevný disk.

3.4.7 Hardwarové a softwarové nároky

Aby mohly být výše zmiňované systémy a aplikace nasazeny, je třeba zhodnotit jejich požadavky na hardware a software. V tabulce 3.4 jsem sepsal jednotlivé požadavky jednotlivých aplikací a systémů. Jedná se o doporučené hodnoty. Nevyplněné buňky ve sloupci HDD znamenají, že požadavek nebyl stanoven.

Co se týče operačního systému u DokuWiki a OTRS nejspíše by byly schopné provozu i na operačním systém Microsoft Windows, ale co se týče mých osobních zkušeností, je lepší je provozovat na operačním systému GNU/Linux. Stejně tak může být nahrazen webový server Apache 2 za Microsoft IIS a MySQL za PostgreSQL.

	CPU	**RAM**	**HDD**	**Operační systém**	**Další požadavky**
Secret Server	2x1.6GHz	2GB		MS Windows XP	IIS, Ms SQL Server 2005
DokuWiki	1x1.6GHz	512MB		GNU/Linux	Apache 2, PHP, MySQL
OTRS	2x2GHz	2GB	160GB	GNU/Linux	Apache 2, Perl, MySQL
Icinga	2x3GHz	4GB	50GB	GNU/Linux	Apache 2, Perl, MySQL
Pohoda	2x2GHz	2GB		MS Windows XP	
Vlastní aplikace	1x1.6GHz	256MB		GNU/Linux	Apache 2, PHP, MySQL

Tabulka 3.4: Seznam doporučeného nebo minimální hardwaru a vyžadovaného softwaru.

3.4.8 Pořizovací cena

Vzhledem k nárokům na hardware a software popsaných v kapitole 3.4.7 Hardwarové a softwarové nároky jsem připravil cenovou kalkulaci na pořízení potřebného hardware a software. Počítal jsem ze začátku se třemi licencemi pro aplikaci Secret Server (já a dva technici). Kalkulace je uvedena v tabulce 3.5. V současnosti již společnost vlastní všechny položky kromě licence na Secret Server.

Zboží	Cena za kus [Kč]	Počet [ks]	Cena [Kč]
HP PL ML110G6 X3430 4G UDIMM 2x500G	12 518	1	12 518
Kingston 4GB 1333MHz ECC Module	803	2	1 606
OEM Windows Server STD 2008 R2 CZ, 5 CAL	12 255	1	12 255
Pohoda Profi (licence pro jednoho uživatele)	7 980	1	7 980
Secret Server (licence pro uživatele)	1 475	3	4 425
Celkem			**38 784**

Tabulka 3.5: Počáteční náklady na pořízení potřebného softwaru a hardwaru (zdroj vlastní).

Kromě počátečních nákladů je třeba také počítat s náklady na podporu a aktualizace pro používaný software. V tabulce 3.6 jsou jednotlivé náklady uvedeny. Včetně výdajů za software, jsou zde i výdaje za umístění serveru v server housingové společnosti. Umístění serveru v server housingové společnosti má několik výhod a to:

- *Fyzickou bezpečnost*: přístup k serveru je neustále hlídán zaměstnanci housingové společnosti. Místnost, kde je server uložen, obsahuje hasící systém bezpečný pro elektroniku.
- *Internetovou konektivitu*: rychlost spojení serveru s internetem je rychlostí 1 Gbps a spojení je zálohováno více linkami.
- *Záložní napájení*: housingová společnost má vlastní výkonné UPS zařízení pro krátké výpadky a diesel agregáty pro dlouhodobé výpadky elektřiny.
- *Klimatizace*: místnost je klimatizována na vhodnou provozní teplotu a vlhkost pro výpočetní techniku.

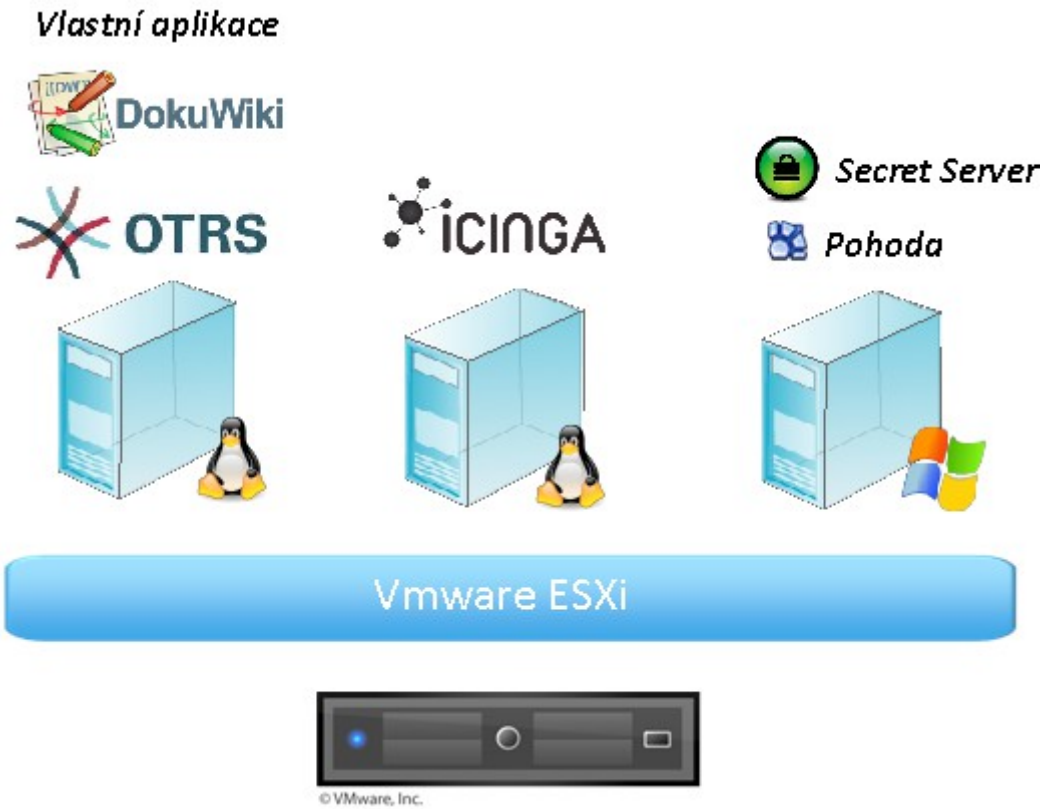
Zboží	Cena za kus [Kč]	Počet [ks]	Cena [Kč]
Secret Server (aktualizace na uživatele)	473	3	1 419
Pohoda Profi (aktualizace)	1 840	1	1 840
Serverhousing (měsíc)	1 420	12	17 040
Celkem			**20 299**

Tabulka 3.6: Roční náklady na provoz a aktualizace softwaru a hardwaru (zdroj vlastní).

Co se týká vlastní aplikace, zde počítám s dobou programování kolem 40 hodin pro potřebnou funkcionalitu. Je samozřejmostí, že s používáním aplikace se najdou další funkce, které budou třeba doprogramovat. Jejich implementaci, budu řešit za běhu, tak jak budou požadavky na aplikaci přicházet.

3.4.9 Implementace

Jelikož byl již vybrán veškerý potřebný software, je třeba rozhodnout se jak proběhne nainstalování na server. Vzhledem k tomu, že některé aplikace vyžadují prostředí Microsoft Windows a jiné GNU/Linux, je třeba více serverů nebo virtualizace. Vzhledem k potřebě nižších nákladů, vyšší efektivity a dostupným nástrojům pro virtualizaci, jsem se rozhodl pro řešení situace právě virtualizací. Výhodou virtualizace je, že ušetříme peníze za pořízení dalšího serveru a na provozních nákladech za housing (případně za elektřinu). Hardware serverů také není ve většině případů efektivně využíván (vytížen), tím že na něj umístíme více virtuálních serverů, které mezi sebou mohou sdílet prostředky, dosáhneme vyšší efektivity.



Ilustrace 3.14: Schéma rozdělení aplikací na počítače.

Pro virtualizaci jsem se rozhodl použít řešení VMware ESXi[22], které je po registraci u společnosti VMware bezplatně dostupné. Toto řešení provádí virtualizaci přímo na hostitelském hardwaru. VMware ESXi má svůj malý minimální kernel, nad

22 Domovská stránka http://www.vmware.com/products/vsphere/esxi-and-esx/overview.html .

kterým virtualizuje. To je podstatný rozdíl oproti řešení VMware Server, které běží nad hostitelským operačním systémem. Nevýhodou produktu VMware ESXi je, že není podporován na každém hardwaru.

Další výhodou virtualizace je nezávislost virtuálních serverů na hostitelském hardwaru, který může být například v případě rozbití hostitelského serveru vyměněn za úplně jiný (v rámci stejné architektury – např. x64, itanium, arm).

Rozdělení aplikací do jednotlivých virtuálních serverů jsem provedl dle ilustrace 3.14. Oddělení aplikace ICINGA od ostatních linuxových aplikací jsem provedl opět na základě osobních zkušeností. Aplikace ICINGA je poměrně rozsáhlá a skládá se z více částí. Jejím oddělením od zbytku získám možnost provádění větších úprav na tomto virtuálním PC, aniž bych ohrozil ostatní systémy. Navíc se tím zvyšuje i bezpečnost celého řešení.

Konfiguraci virtuálních serverů jsem se rozhodl provést dle tabulky 3.7. Jak je z tabulky patrné, nevyužil jsem veškeré dostupné prostředky fyzického serveru, protože mám v budoucnu plán na server přidat další virtuální servery.

Název serveru	**OS**	**CPU**	**RAM**	**HDD**
v1	Windows Server 2008 R2 STD	2x2,39GHz	4GB	80GB
v2	GNU/Linux Debian Squeeze	2x2,39GHz	2GB	60GB
v3	GNU/Linux Debian Squeeze	2x2,39GHz	2GB	60GB

Tabulka 3.7: Konfigurace virtuálních serverů (zdroj vlastní).

Virtuálním serverům jsem přiřadil méně diskového prostoru, než je uvedeno v doporučené konfiguraci zobrazené v tabulce 3.4. Učinil jsem tak na základě zkušeností a skutečnosti, že disky fyzického serveru nejsou příliš velké. Pokud by se v budoucnosti ukázalo, že je některému virtuálnímu serveru přiřadit více místa, je možné disk bez ztráty dat rozšířit.

4 ISMS

Společnost si uvědomuje míru citlivosti dat, která o svých zákaznících spravuje, zejména v případě přístupových údajů. Společnost má s těmito přístupovými údaji neomezený přístup k datům svých zákazníků, je proto velice důležité stanovit a udržovat adekvátní bezpečnostní opatření.

Cílem kapitoly nemá být kompletní příprava k certifikaci dle normy ČSN ISO/IEC 27001. V kapitole mi jde hlavně o zjištění, jak si navržené řešení stojí, a zlepšení bezpečnosti navrženého řešení aplikováním vhodných opatření.

Obsahem této kapitoly je:

- identifikace aktiva,
- identifikace možných hrozeb a zranitelností,
- výběr a aplikování vhodných opatření,
- vyhodnocení velikosti rizika hrozeb na aktiva.

4.1 Rozsah ISMS

Na základě posouzení specifických rysů činnosti společnosti, jejího uspořádání, struktury, aktiv a technologií jsem se rozhodl omezit rozsah ISMS pouze na informační aktiva.

Společnost má minimální hmotný majetek, jeho ztráta a poškození nemá pro společnost příliš velký dopad. Na rozdíl od hmotného majetku spravuje společnost velké množství důvěrných informací, jejichž ztráta nebo zveřejnění by mohlo mít na společnost likvidační následky.

4.2 Metoda hodnocení rizik

Pro hodnocení dopadu ztráty důvěrnosti, integrity a dostupnosti aktiv jsem se rozhodl využít stupnici z tabulky 4.1. Pro celkové hodnocení dopadu jsem se rozhodl sečíst dílčí dopady, přičemž nízké hodnocení bylo zastoupeno jedním bodem, střední dvěma body a vysoké hodnocení třemi body.

Hrozby budou hodnoceny součtem rizika jednotlivých zranitelností, přičemž riziko zranitelnosti bude součinem dopadu na podnikání a pravděpodobnosti incidentu využívajícího danou zranitelnost. Pravděpodobnost je hodnocena na stupnici od nuly do jedné, stejně jako se pravděpodobnost vyjadřuje v matematice. Dopad na podnikání se vyjadřuje na stupnici od nuly do desíti, přičemž:

- nula: žádný dopad,
- jedna: ztráty v řádu stovek korun,
- pět: ztráty v řádu desítek tisíc korun, poškození dobrého jména společnosti,
- deset: ztráty v řádu statisíců korun, zánik splečnosti.

Riziko aktiva jsem se rozhodl vypočítat součinem výsledného rizika hrozby a velikosti dopadu ztráty důvěrnosti, integrity nebo dostupnosti aktiva, podle toho, co hrozba způsobuje.

Impact of Loss ►	LOW	MEDIUM	HIGH
Confidentiality Ensuring that information is accessible only to those authorized to have access	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Safeguarding the accuracy and completeness of information and processing methods	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring that authorized users have access to information and associated assets when required	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Tabulka 4.1: Stupnice pro hodnocení aktiv (zdroj „ISMS Implementation Guide“[10]).

4.3 Identifikace aktiv, hrozeb a zranitelností

Nejprve je třeba identifikovat aktiva v rozsahu, jak to stanovuje kapitola 4.1 Rozsah ISMS. Identifikovaná aktiva jsem zaznamenal v tabulce č. 4.2 včetně jejich popisu, vlastníka aktiva a umístění aktiva.

Aktivum	Popis	Vlastník	Umístění
Databáze znalostí	Dokumentace postupů a ICT prostředí zákazníků.	Vedoucí technik	Brno – dat. centrum
Databáze incidentů	Seznam všech provedených prací.	Vedoucí technik	Brno – dat. centrum
Databáze hesel	Seznam všech hesel do firemních systémů a systémů zákazníků.	Jednatel	Brno – dat. centrum
Účetnictví	Účetnictví firmy dle zákona o učetnictví (zákon č. 563/1991 Sb.)	Účetní	Brno – dat. centrum
Elektronická pošta	Mailový systém vč. samotných e-mailů.	Jednatel	Google Apps

Tabulka 4.2: Seznam identifikovaných informačních aktiv (zdroj vlastní).

Pro identifikovaná aktiva jsem následně stanovil velikost dopadu na ztrátu důvěrnosti, integrity a dostupnosti těchto aktiv (viz tabulka č. 4.3). Hodnocení probíhalo dle kapitoly 4.2 Metoda hodnocení rizik. Celkové dopad byl pak stanoven sečtením všech tří dílčích velikostí dopadu.

Aktivum	Dopad ztráty			Celkový dopad
	Důvěrnosti	Integrity	Dostupnosti	
Databáze znalostí	Střední	Střední	Nízký	5
Databáze incidentů	Střední	Střední	Střední	6
Databáze hesel	Vysoký	Vysoký	Střední	8
Účetnictví	Nízký	Vysoký	Nízký	5
Elektronická pošta	Střední	Nízký	Střední	5

Tabulka 4.3: Hodnocení velikosti dopadu na ztrátu důvěrnosti, integrity a dostupnosti pro jednotlivá aktiva (zdroj vlastní).

Dále jsem provedl identifikaci možných hrozeb a jejich zranitelností. Pro každou zranitelnost jsem vybral a aplikoval opatření dle přílohy A normy ČSN/ISO IEC 27001. Opatření jsem vybíral dle svého úsudku, přičemž jsem kladl důraz na co nejlepší poměr nákladů na zavedení a udržení opatření a jeho přínosy. V tabulce č. 4.5 jsou uvedena opatření pro hrozbu ztráty důvěrnosti aktiva, v tabulce č. 4.4 pro hrozbu ztráty integrity aktiva a v tabulce č. 4.6 pro hrozbu ztráty dostupnosti. Každá tabulka obsahuje kromě

Hrozba	Zranitelnost		Aplikovaná opatření	Pravděpodobnost výskytu	Velikost dopadu na podnikání	Výsledné hodnocení
	Kdo	Jak				
Ztráta důvěrnosti aktiva						0,900
	zaměstnanci					0,400
		úmyslně	8.1.3 , 8.3.3, 10.1.3	0,030	8	0,240
		neúmyslně	8.2.1, 10.1.3, 10.8.1, 11.7.1	0,040	4	0,160
	spolupracující subjekty					0,120
		úmyslně	6.2.X, 8.3.3	0,010	6	0,060
		neúmyslně	8.1.3, 10.8.1	0,020	3	0,060
	dodavatelé					0,050
		úmyslně	6.2.X, 8.3.3	0,010	3	0,030
		neúmyslně	8.1.3, 10.8.1	0,020	1	0,020
	zákazníci					0,090
		úmyslně	6.2.X, 8.3.3	0,010	5	0,050
		neúmyslně	8.1.3, 10.8.1	0,020	2	0,040
	ostatní					0,240
		fyzická krádež dat	9.1.1,9.2.1	0,010	8	0,080
		elektronická krádež dat	10.3.2, 10.6.1, 11.3.1	0,020	8	0,160

Tabulka 4.5: Seznam zranitelností, jejich opatření a rizika pro hrozbu ztráty důvěrnosti aktiva (zdroj vlastni).

Hrozba	Zranitelnost		Aplikovaná opatření	Pravděpodobnost výskytu	Velikost dopadu na podnikání	Výsledné hodnocení
	Kdo	Jak				
Modifikace nebo ztráta aktiva						0,357
	vyšší moc					0,112
		požár	9.1.4, 10.5.1	0,002	8	0,016
		přírodní katastrofa	9.1.4, 10.5.1	0,010	8	0,080
		občanské nepokoje, válka	9.1.4, 10.5.1	0,002	8	0,016
	zaměstnanci					0,050
		úmyslně	8.1.3, 8.3.3, 10.1.3, 10.5.1	0,010	3	0,030
		neúmyslně	8.2.1, 10.1.3, 10.5.1, 11.7.1	0,020	1	0,020
	spolupracující subjekty					0,090
		úmyslně	6.2.X, 8.3.3	0,010	5	0,050
		neúmyslně	8.1.3, 10.5.1	0,020	2	0,040
	dodavatelé					0,018
		úmyslně	6.2.X, 8.3.3	0,008	1	0,008
		neúmyslně	8.1.3, 10.5.1	0,010	1	0,010
	zákazníci					0,080
		úmyslně	6.2.X, 8.3.3	0,010	4	0,040
		neúmyslně	8.1.3, 10.5.1	0,020	2	0,040
	ostatní					0,007
		fyzické zničení dat	9.1.1, 9.2.1, 10.5.1	0,001	2	0,002
		elektronické smazání dat	10.5.1, 10.6.1, 11.3.1	0,005	1	0,005

Tabulka 4.4: Seznam zranitelností, jejich opatření a rizika pro hrozbu ztráty integrity aktiva (zdroj vlastní).

Hrozba	Zranitelnost		Aplikovaná opatření	Pravděpodobnost výskytu	Velikost dopadu na podnikání	Výsledné hodnocení
	Kdo	Jak				
Znepřístupnění aktiva						0,360
	zaměstnanci					0,030
		úmyslně	8.1.3, 8.3.3, 10.1.3	0,010	2	0,020
		neúmyslně	10.1.3	0,010	1	0,010
	ostatní					0,330
		výpadek el. proudu	9.2.2	0,005	3	0,015
		výpadek konektivity	9.2.2	0,005	1	0,005
		porucha HW	9.2.2	0,050	4	0,200
		škodlivý software	10.3.2, 10.6.1	0,010	4	0,040
		elektronický útok	10.3.2, 10.6.1	0,010	4	0,040
		přetížení	10.3.1	0,010	3	0,030

Tabulka 4.6: Seznam zranitelností, jejich opatření a rizika pro hrozbu ztráty dostupnosti aktiva (zdroj vlastni).

zranitelností i seznam aplikovaných opatření, odhad pravděpodobnosti výskytu incidentu zneužívajícího danou zranitelnost a možný dopad na podnikání.

Jelikož jsou některá opatření aplikována proti více zranitelnostem, sestavil jsem tabulku č. 4.7 se soupisem všech použitých opatření, včetně odkazu na místo kde je opatření dokumentováno.

Číslo	Název	Místo dokumentování
6	Organizace bezpečnosti informací	
6.2	Externí subjekty	Bezpečnostní politika
6.2.1	Identifikace rizik plynoucích z přístupu externích subjektů	
6.2.2	Bezpečnostní požadavky pro přístup klientů	
6.2.3	Bezpečnostní požadavky v dohodách se třetí stranou	
8	Bezpečnost lidských zdrojů	
8.1	Před vznikem pracovního vztahu	Bezpečnostní politika
8.1.3	Podmínky výkonu pracovní činnosti	
8.2	Během pracovního vztahu	Bezpečnostní politika
8.2.1	Odpovědnost vedoucích zaměstnanců	
8.3	Ukončení nebo změna pracovního vztahu	Bezpečnostní politika
8.3.3	Odebrání přístupových práv	
9	Fyzická bezpečnost a bezpečnost prostředí	
9.1	Zabezpečené oblasti	Bezpečnostní opatření
9.1.1	Fyzický bezpečnostní perimetr	
9.1.4	Ochrana před hrozbami vnějšku a prostředí	
9.2	Bezpečnost zařízení	Bezpečnostní opatření
9.2.1	Umístění zařízení a jeho ochrana	
9.2.2	Podpůrná zařízení	
10	Řízení komunikací a řízení provozu	
10.1	Provozní postupy a odpovědnosti	Bezpečnostní politika
10.1.3	Oddělení povinností	
10.3	Plánování a přejímání systémů	Bezpečnostní opatření
10.3.1	Řízení kapacit	
10.3.2	Přejímání systémů	
10.5	Zálohování	Bezpečnostní opatření
10.5.1	Zálohování informací	
10.6	Správa bezpečnosti sítě	Bezpečnostní opatření
10.6.1	Síťová opatření	
10.8	Výměna informací	Bezpečnostní politika
10.8.1	Postupy a politiky při výměně informací	
11	Řízení přístupu	
11.3	Odpovědnosti uživatelů	Bezpečnostní politika
11.3.1	Používání hesel	
11.7	Mobilní výpočetní zařízení a práce na dálku	Bezpečnostní politika
11.7.1	Práce na dálku	

Tabulka 4.7: Seznam použitých opatření (zdroj vlastní).

4.4 Bezpečnostní politika

Tato kapitola obsahuje závazné pokyny, kterými se musí zaměstnanci společnosti řídit. Tyto pokyny vznikly na základě vybraných opatření z přílohy A normy ČSN/ISO IEC 27001 a navržených firemních procesů v kapitole 3.3 Navrhované řešení. Pokyny budou pro interní použití publikované v databázi znalostí. Pokyny jsou tříděny dle subjektu, na který se vztahují.

4.4.1 Zaměstnanci

Tato kapitola obsahuje pokyny vztahující se k zaměstnancům společnosti.

4.4.1.1 Vznik pracovně právního vztahu (8.1, 10.1.3)

Případní zaměstnanci společnosti jsou vybíráni na základě doporučení a ústního pohovoru s jednatelem společnosti. V případě potřeby jsou jejich znalosti ověřeny praktickým testem.

S každým zaměstnancem je podepsána pracovní smlouva. Tato smlouva musí zajistit mlčenlivost zaměstnanců o důvěrných informacích a zabránit v odchodu zákazníků spolu se zaměstnancem.

Zaměstnanci jsou vedoucím technikem vytvořeny přístupové účty a zpřístupněny informace, které bude dle svého pracovního zařazení potřebovat.

4.4.1.2 Ukončení pracovně právního vztahu (8.3)

V případě ukončení pracovně právního vztahu musí být odcházející zaměstnanec poučen o svých povinnostech. Zejména o povinnosti mlčenlivosti o důvěrných informacích a zdržení se nekalé činnosti (přetažení zákazníků nebo zaměstnanců).

Odcházejícímu zaměstnanci musí být vedoucím technikem zrušeny veškeré přístupy, ke kterým již nemá mít přístup (informační systém, aplikace, VPN atd.).

Zaměstnanec musí jednateli společnosti vrátit veškeré svěřené vybavení a klíče.

4.4.1.3 Odpovědnost vedoucích zaměstnanců (8.2.1)

Vedoucí zaměstnanci jsou odpovědní za své podřízené. Je jejich povinností dohlížet a případně kontrolovat, zda jim podřízení zaměstnanci dodržují bezpečnostní

pravidla a pracovní postupy i doporučení. V případě zjištění nedostatků nebo drobných chyb je v jejich kompetenci sjednat nápravu. O závažných pochybeních musí být informován jednatel společnosti.

4.4.1.4 Výměna informací (10.8.1)

Je-li potřeba vyměnit si s někým důvěrné informace, budou tyto informace zašifrovány komprimačním programem. Zašifrovaný archiv bude odeslán elektronickou poštou (e-mailem) a heslo k archivu přes SMS. Není-li možné využít výše uvedený postup z důvodu velikosti archivu, může být šifrovaný archiv distribuován přes firemní server.

Alternativně lze informace předat osobně přes paměťové médium (CD, DVD, USB Flash paměť, HDD atd.).

4.4.1.5 Používání hesel (11.3.1)

Tvorba a používání hesel se řídí níže uvedenými pravidly.

- Používaná hesla musí být unikátní, není možné použít stejné heslo pro více účtů.
- Všechna hesla musí být uložena v databázi hesel.
- Pokud je to možné, je pro generování hesel třeba použít databázi hesel
- Každé heslo musí být dlouhé alespoň 8 znaků a obsahovat malá i velká písmena a číslice. Heslo může volitelně obsahovat speciální znaky.

4.4.1.6 Práce na dálku (11.7.1)

U jakékoliv síťové komunikace obsahující důvěrné informace je zaměstnanec povinen využít šifrování této komunikace nebo zabezpečeného kanálu (např. VPN, SSH tunneling), tak aby bylo překonáno nezabezpečené prostředí (internet, nefiremní WIFI atd.).

4.4.2 Externí subjekty

Tato kapitola řeší pokyny pro navazování a ukončování vztahů s dodavateli, zákazníky a spolupracujícími subjekty.

4.4.3 Před zahájením spolupráce (6.2, 8.1.3)

Vždy před zahájením spolupráce s konkrétním externími subjektem (dodavatelé, zákazníci a spolupracující subjekty) je třeba identifikovat, k jakým informacím potřebuje přístup a jaké z toho plynou hrozby.

Je třeba vyhodnotit smysluplnost přístupu k požadovaným informacím a připravit přístupové účty s co možná nejmenšími oprávněními. Se subjektem se dohodnou bezpečnostní opatření a jejich dodržování musí být vyžadováno smlouvou.

Smlouva, uzavíraná se subjektem, musí pokrývat veškeré relevantní bezpečnostní požadavky a stanovovat smluvní pokuty za jejich porušení.

4.4.3.1 Ukončení spolupráce (8.3.3)

Při ukončení spolupráce s externím subjektem, je povinností vedoucího technika zrušit všechny přístupové účty, přidělené konkrétnímu subjektu. Jednatel společnosti zároveň upozorní externí subjekt o povinnosti smazání získaných informací a dodržování mlčenlivosti, pokud nebylo ve smlouvě uvedeno jinak.

4.4.3.2 Výměna informací (10.8.1)

Způsob výměny bude zvolen dle povahy vyměňovaných informací. Pro jejich výměnu může sloužit již existující firemní informační systém, nebo mohou být použity stejné metody jako v případě kapitoly 4.4.1.4 Výměna informací (10.8.1).

4.5 Bezpečnostní opatření

Tato kapitola popisuje aplikovaná bezpečnostní opatření stejně jako kapitola 4.4 Bezpečnostní politika, ovšem tato opatření jsou, dle mého názoru, více specifická a není zatím vhodné je zařazovat do bezpečnostní politiky.

4.5.1 Informační systém – SW

Níže uvedená bezpečnostní opatření se vztahují k softwarové části firemního informačního systému.

4.5.1.1 Plánování a přejímání systémů (10.3)

Všechny servery jsou monitorovány automatickým monitorovacím systémem ICINGA. Tento systém, kromě jiného, měří vytížení serverů (disku, procesoru, paměti atd.) a poskytuje nám přehled o vývoji vytížení. Díky tomu jsme schopni identifikovat kapacitní nedostatky serverů a včas provést vhodná opatření.

U aplikací a systémů, které jsou součástí firemního informačního systému, pravidelně automatizovaně aplikujeme bezpečnostní aktualizace. V případě vydání nové verze aplikace nebo systému je nejprve rozhodnuto, zda je vhodné aktualizaci provést a jak rychle. Následná aktualizace nejprve probíhá v testovacím prostředí a po základním ověření funkčnosti je nasazena do produkčního prostředí.

4.5.1.2 Zálohování (10.5)

Všechna data informačního systému jsou každý den automaticky zálohována. Zálohování je prováděno na další firemní server, který je určen pouze k ukládání zálohovaných dat. Zálohovaná data se uchovávají alespoň po dobu 14 dnů.

4.5.1.3 Síťová opatření (10.6)

Operační systémy serverů (fyzických i virtuálních) jsou pravidelně automaticky aktualizovány, aby byla minimalizována pravděpodobnost proniknutí do serveru pomocí známé bezpečnostní chyby.

Při konfiguraci operačních systémů a služeb se vychází z našich zkušeností i znalostí a pravidla „co není povoleno, je zakázáno“. Každý operační systém má nastaven firewall. Pokud je to možné, je pro síťovou komunikaci vždy využito šifrování. Nepotřebné a nepoužívané aplikace jsou vždy odinstalovány.

4.5.2 Informační systém – HW

Níže uvedená bezpečnostní opatření se vztahují k hardwarové části firemního informačního systému.

4.5.2.1 Zabezpečené oblasti (9.1)

Servery, jež slouží k provozu informačního systému a ukládání informací, jsou umístěny u společnosti Master Internet, s.r.o. v brněnské pobočce. Tato společnost

vlastní datová centra a zabývá se pronájmem serverů a poskytováním místa pro provozování serverů v jejich datových centrech.

Prostory datového centra jsou kamerově monitorovány a na místě je neustále přítomen dozor. Přístup do datového centra je protokolován a vpuštěny jsou pouze autorizované osoby.

Datové centrum je pro případ požáru vybaveno plynovým hasícím systémem, který v případě použití nepoškozuje elektroniku.

Případné povodně nebo záplavy by neměly datové centrum poškodit, protože se nachází v pátém nadzemním podlaží.

4.5.2.2 Bezpečnost zařízení (9.2)

Proti neoprávněnému přístupu jsou zařízení chráněna umístěním v datovém centru (viz předchozí kapitola).

V případě výpadku elektrického proudu je datové centrum vybaveno záložními bateriovými zdroji. Pro případ dlouhodobého výpadku je datové centrum vybaveno dieselovými motorgenerátory.

Připojení k internetu (konektivita) je realizováno několika nezávislými přívody optických vláken.

Dodržování doporučené provozní teploty a relativní vlhkosti je zaručeno zálohovaným klimatizačním systémem datového centra.

4.6 Výsledné hodnocení

Na základě metody hodnocení rizik rozebrané v kapitole 4.2 Metoda hodnocení rizik a identifikovaných aktiv, hrozeb a opatření v kapitole 4.3 Identifikace aktiv, hrozeb a zranitelností jsem sestavil tabulku č. 4.8 s výsledným hodnocením. Buňky s výsledným rizikem jsem, pro vyšší přehlednost, obarvil dle velikosti rizika.

Z tabulky vyplývá, že největší hrozbou je ztráta důvěrnosti, obzvláště u databáze hesel. Pro hrozbu ztráty důvěrnosti budu muset v budoucnu aplikovat další opatření. Ostatní hrozby jsou dle mého názoru v akceptovatelných mezích a zbytkové riziko bude moci být akceptováno.

Aktivum	Hrozba	Riziko hrozby	Dopad na aktivum	Výsledné riziko
Databáze znalostí	Ztráta důvěrnosti	0,900	2	1,800
	Ztráta integrity	0,357	2	0,714
	Ztráta dostupnosti	0,360	1	0,360
Databáze incidentů	Ztráta důvěrnosti	0,900	2	1,800
	Ztráta integrity	0,357	2	0,714
	Ztráta dostupnosti	0,360	2	0,720
Databáze hesel	Ztráta důvěrnosti	0,900	3	2,700
	Ztráta integrity	0,357	3	1,071
	Ztráta dostupnosti	0,360	2	0,720
Účetnictví	Ztráta důvěrnosti	0,900	1	0,900
	Ztráta integrity	0,357	3	1,071
	Ztráta dostupnosti	0,360	1	0,360
Elektronická pošta	Ztráta důvěrnosti	0,900	2	1,800
	Ztráta integrity	0,357	1	0,357
	Ztráta dostupnosti	0,360	2	0,720

Tabulka 4.8: Výsledné hodnocení rizik pro jednotlivá aktiva (zdroj vlastní).

5 ITSM

V této kapitole se chci věnovat vyhodnocení souladu mnou navržených procesů oproti požadavkům normy ČSN ISO/IEC 20000-1:2006. Cílem není, aby procesy byly v naprostém souladu, ale zjištění, jak si procesy stojí a případně provést úpravy procesů, které by při nízkých nákladech přinesly výrazné zkvalitnění.

5.1 Katalog služeb

V kapitole 2.2.2 Katalog služeb jsem již rozebíral služby nabízené zákazníkům, avšak tehdy to bylo z pohledu obchodního. V této kapitole, bych chtěl krátce prezentovat katalog služeb z technického hlediska. Katalog je uveden v tabulce 5.1 a vychází ze seznamu procesů z kapitoly 3.3.2 Přehled procesů.

Služba	**Popis**
Servis	Odstraňování závad a problémů v zákazníkově ICT síti, změny v konfiguraci, instalace aplikací. Například instalace nového PC, vytvoření e-mailu nebo odvirování PC.
Pravidelná kontrola	Pravidelné kontrolování zákazníkova ICT prostředí technikem zda je vše v pořádku a nevykazuje odchylky od dokumentovaného stavu. Například kontrola nainstalovaného softwaru, aktualizací nebo zabezpečení.
Změna v ICT síti	Proces provádění větších změn v zákazníkově ICT síti. Například migrace serveru, změna informačního systému, modernizace sítě.
Dodání HW a SW	Proces zajištění dodávky HW a SW na přání zákazníka (od nákupu až po dodání a zprovoznění).
Monitorování serveru	Nepřetržité kontrolování serverů zákazníků, jimi poskytovaných služeb a vytížení. Například zda server není nedostupný.

Tabulka 5.1: Katalog služeb z technického hlediska (zdroj vlastní).

5.2 Procesy managementu služeb

V podkapitolách této kapitoly, budu procházet jednotlivé procesy managementu služeb, tak jak jsou stanoveny v normě ČSN ISO/IEC 20000-1:2006. U každého procesu popíši jak navržené firemní procesy naplňují požadavky stanovené normou.

5.2.1 Management úrovně služeb (6.1.)

Všechny běžně dodávané služby společnosti jsou uvedeny ve veřejně přístupném katalogu služeb na webových stránkách společnosti. V této práci jsou poskytované

služby rozepsány v kapitole 2.2.2 Katalog služeb po obchodní stránce (tak jak jsou prezentovány zákazníkům) a kapitole 5.1 Katalog služeb po technické stránce (z čeho se služba skládá).

Součástí každé smlouvy uzavírané se zákazníkem je i ujednání o úrovni poskytovaných služeb (SLA). Ujednání o úrovni poskytovaných služeb obsahuje seznam poskytovaných služeb, jejich popis, záruky a podmínky za jakých jsou služby poskytovány.

Konkrétní podoba ujednání o úrovni poskytovaných služeb je pro každého zákazníka připravována na míru. Tato ujednání jsou pravidelně revidována, aby byla zajištěna jejich aktuálnost trendům a potřebám zákazníkům.

5.2.2 Výkazy o službách (6.2.)

Navržený firemní informační systém umožňuje tvorbu výkazů, které se používají pro kvalifikované rozhodování, plánování a efektivní komunikaci. V současné době umožňuje firemní informační systém tvorbu následujících výkazů:

- výkaz o incidentech (rozlišitelný dle času a zákazníka),
- výkaz o práci techniků,
- výkaz o souladu a nesouladu s SLA (rozlišitelný dle zákazníka a incidentu).

Z těchto výkazů jsme schopni splnit všechny požadavky na výkazy stanovené v normě. Výkazy o plnění úrovně poskytovaných služeb jsou každý měsíc vytvářeny a odesílány spolu s výkazem práce (výkazem o incidentech) zákazníkům. Co se týče ostatních výkazů, ty jsou v současné době tvořeny na nepravidelné bázi a pouze pro vnitřní potřebu společnosti.

5.2.3 Management kontinuity a dostupnosti služeb (6.3.)

Vzhledem k aktuálnímu počtu zaměstnanců a finančním možnostem společnosti, jsem se rozhodl tuto problematiku neřešit. Tuto problematiku přesto pokládám za důležitou a při dosažení vyššího počtu zaměstnanců a vyšší finanční stability společnosti se k ní vrátím, abych management dostupnosti služeb definoval.

5.2.4 Rozpočtování a účtování pro IT služby (6.4.)

Jak jsem již psal v kapitole 5.2.2 Výkazy o službách (6.2.), náš informační systém uchovává údaje o poskytnutých službách a jejich cenách. Tyto informace jsou následně s každou fakturou zasílány zákazníkům.

Tím mají zákazníci detailní přehled za co kolik platí. Tyto výkazy jsou z naší strany archivovány a je možné se k nim v případě pochybností kdykoliv vrátit.

5.2.5 Management kapacit (6.5.)

Stejně jako v kapitole 5.2.3 Management kontinuity a dostupnosti služeb (6.3.) jsem se rozhodl tuto oblast neřešit. Je samozřejmostí, že mám představu o kapacitách, využití a možnostech lidských zdrojů, ale to nestačí na to, abych tuto oblast managementu zaváděl. K této oblasti se vrátím v budoucnu.

5.2.6 Management bezpečnosti informací (6.6.)

Je nutné stanovit jednotný a jednoznačný systém odpovědnosti, zajistit důvěryhodnost, integritu, dostupnost a účtovatelnost při práci s daty. Společnost se svými zákazníky podepisuje dohodu o mlčenlivosti podléhající smluvním pokutám. Je proto v jejím zájmu, aby s daty nebylo nakládáno neoprávněným způsobem. Na druhou stranu, čím vyšší zabezpečení dat, tím vyšší náklady na dosažení a udržení dané úrovně. Proto se společnost snaží držet kolem bodu, kdy jsou náklady na zabezpečení rovny velikosti dopadu rizika.

Blíže se problému řízení bezpečnosti informací věnovala kapitola 4 ISMS.

5.2.7 Management vztahů s byznysem (7.2.)

Dosavadní růst společnosti přisuzuji vynikajícímu vztahu s byznysem a udržení těchto vztahů je pro nás naprosto esenciální.

Každý rok před svátky jsou všichni zákazníci navštíveni jednatelem společnosti (mnou) v duchu polo-formálního setkání, kde je jim poděkováno (slovně a materiálně) za spolupráci v minulém roce a jsou probrány výhledy na další rok. V případě potřeby mohou zákazníci kdykoliv požádat o obchodní schůzku a jejich potřeby i přání budou probrány a realizovány (např. úpravy smluv, úrovní služeb, poskytovaných služeb).

Každý zákazník má přiřazeného osobního technika, který je zákazníkovým primárním kontaktem a řeší s ním veškeré technické záležitosti. Tímto se snažíme budovat důvěru a vztah mezi zákazníkem a společností.

Proces stížností není formálně definován. Nicméně vzhledem k tomu, že každý zákazník se zná osobně s jednatelem společnosti, může se na něj kdykoliv obrátit a jednatel společnosti se postará o vyřešení stížnosti k zákazníkově spokojenosti.

5.2.8 Management vztahu s dodavateli (7.3.)

Společnost má pouze několik dodavatelů. Jedná se o dodavatele hardwaru a softwaru a dodavatele poskytujícího housing serverů.

Co se týče dodavatelů hardwaru a softwaru, těch je v České republice dostatek a společnost spolupracuje s pěti největšími. Jejich sortiment je převážně stejný, takže si společnost může vybírat dodavatele dle ceny a skladové dostupnosti konkrétního HW a SW. Společnost však nemá vyjednávací sílu, aby si vyjednala nějaké nestandardní podmínky. S těmito dodavateli není uzavřena smlouva o úrovni služeb.

Vztah s dodavatelem housingu serverů je řízen dle jeho standardních smluvních podmínek, za kterých poskytuje danou službu. Společnost je pro něj příliš malým partnerem, aby si mohla nárokovat osobní přístup, proto ani smlouva o úrovni služeb nenese příliš garancí.

V souhrnu se dá říci, že společnost má s dodavateli dobrý vztah. V případě selhání dodavatelů však nemá žádné páky, jak by mohla vymáhat kompenzaci vzniklé škody.

5.2.9 Management incidentů (8.2.)

Pro správu incidentů slouží část informačního systému nazývaná databáze incidentů (viz 3.3.3.1 Databáze incidentů). Každý nahlášený incident je do databáze ihned zaznamenán a je mu přiřazen vlastník i priorita. Při stanovování priority se vychází z ilustrace 5.1. Hodnota v matici je vždy dána součtem hodnost na osách.

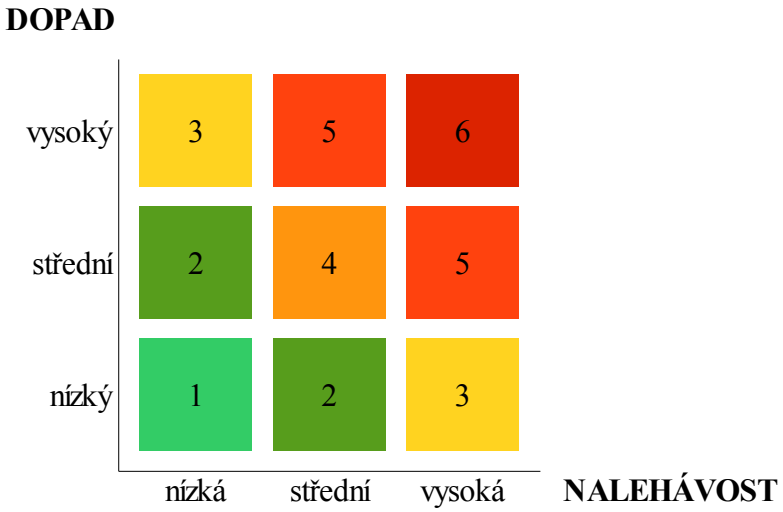
Incidenty jsou vždy řešeny dle procesu „Servis“ viz kapitola 3.3.4.2 Servis. Tento proces v sobě již zahrnuje požadavky normy:

- zaznamenávání a archivaci incidentů,
- řešení incidentu ve spolupráci s databází znalostí,

- aktualizování o průběhu incidentu,
- informování stanovených osob (včetně zákazníka),
- komunikaci se zákazníkem,
- formální uzavření incidentu.

Hierarchie pro eskalaci problému je následující (od nejnižší úrovně po nejvyšší):

- osobní technik,
- vedoucí technik,
- jednatel společnosti.



Ilustrace 5.1: Tříbodouvá stupnice pro hodnocení priority (zdroj vlastní).

5.2.10 Management problémů (8.3.)

Aktivní přístup k předcházení problémů je zajištěn pomocí procesu pravidelných kontrol viz kapitola 3.3.4.3 Pravidelná kontrola. Proces zajišťuje pravidelnou kontrolu zákazníkova ICT prostředí spravovaného naší společností. Proces „Pravidelná kontrola“ hlavně kontroluje stav zabezpečení prostředí, soulad prostředí s dokumentací a uzavřenou smlouvou. V případě identifikace incidentu nebo nové hrozby jsou ihned prováděny nápravné akce.

S problémy (tak, jak jsou definovány normou) je zacházeno stejně jako s incidenty, tzn. jsou zaznamenány v databázi incidentů a řešeny co nejdříve, aby byly minimalizovány jejich možné dopady.

U problémů, u kterých existuje možnost, že by se mohly objevit i někdy v budoucnu, je vytvořen záznam v databázi znalostí. Tento záznam popisuje problém, jeho příznaky a možná řešení.

5.2.11 Management konfigurací (9.1.)

Konfigurace služeb je stanovena v technickém katalogu služeb a databázi znalostí. V technickém katalogu služeb jsou služby vymezeny obsahově. V databázi znalostí jsou shromážděny směrnice, doporučení a nejlepší praktiky jak služby poskytovat. Všechny položky v databázi znalostí jsou jednoznačně identifikovatelné, veškeré změny jsou auditovány a je možné se vracet ke starším verzím.

V databázi znalostí jsou také konfigurace služeb pro každého zákazníka. Konfigurace se skládá z části, kde jsou popsány poskytované služby a části, kde je popsána konfigurace zákazníkova ICT prostředí.

Samozřejmostí je také napojení databáze znalostí na databázi incidentů. Je tedy možné v dokumentaci konfigurace sledovat vliv jednotlivých incidentů nebo problémů na konfiguraci.

5.2.12 Management změn (9.2.)

Změny v konfiguraci prostředí zákazníků jsou prováděny osobními techniky v případě, že pro změnu existuje návod v databázi znalostí. Jestliže návod v databázi znalostí neexistuje, musí provést schválení vedoucí technik a návod případně vypracovat. Změny v konfiguraci jsou následně zaznamenány v databázi znalostí.

Změny v konfiguraci služeb zákazníků může provádět obchodník nebo jednatel společnosti. Veškeré změny jsou následně zaznamenány v informačním systému společnosti.

Úpravy konfigurace v ICT prostředí firmy jsou v režii vedoucího technika. On je zodpovědný za jejich schvalování a osobní implementaci. Pokud to charakter změny umožňuje, může implementaci změny delegovat na technika. Změny konfigurace jsou opět zaznamenány v databázi znalostí.

5.2.13 Management uvolnění (10.1.)

Veškeré změny v konfiguraci se převádí do praxe dle zvážení odpovědně osoby nebo přání zákazníka a není stanoven žádný pevný cyklus.

Změny v konfiguraci prostředí zákazníků jsou prováděny na jejich žádost, nebo jako preventivní opatření na doporučení osobního technika či výsledek pravidelné kontroly. Pokud to charakter změny umožňuje, jsou aplikovány přímo do produkčního prostředí. V opačném případě je sestaveno testovací prostředí, nebo jsou změny zavedeny v pilotním režimu. Termín provedení změn závisí na přání zákazníka a vytíženosti technika, který bude zodpovědný za realizaci změny.

Ke změnám v konfiguraci služeb zákazníka dochází na jeho žádost a schválení obchodníkem, nebo na doporučení obchodníka a schválení zákazníkem. V krajním případě může být provedena změna konfigurace služeb jednostranně (například vypovězení smlouvy).

Úpravy v prostředí společnosti jsou prováděny na základě doporučení všech zaměstnanců společnosti. Nejprve však musí dojít k diskuzi nad doporučovanou úpravou na schůzce vedení společnosti (vedoucí technik, obchodník a jednatel) a v případě jejího schválení je vybrána vhodná metoda zavádění a změna implementována.

5.3 Soulad implementovaných procesů managementu služeb s normou ČSN ISO/IEC 20000-1:2006

V tabulce 5.2 jsem se pokusil shrnout soulad výše zmíněných procesů s normou a v případě nesouladu napsat důvod nesouladu. Z tabulky vyplývá, že mnou navržené procesy jsou spíše v souladu s normou.

Výsledky je však třeba brát s rezervou, jelikož hodnocení souladu s normou jsem prováděl sám a výsledky nebyly konzultovány s auditorem.

Procesy dodávky služeb dle ČSN ISO/IEC 20000-1:2006		**Implementováno**
6.	Procesy dodávky služeb	
6.1.	Management úrovně služeb	ano
6.2.	Výkazy o službách	ano
6.3.	Management kontinuity a dostupnosti služeb	ne
	Z důvodu nízkého počtu zaměstnanců a finančních možností společnosti.	
6.4.	Rozpočtování a účtování pro IT služby	ano
6.5.	Management kapacit	ne
	Z důvodu nízkého počtu zaměstnanců a finančních možností společnosti.	
6.6.	Management bezpečnosti informací	částečně
	Viz kapitola ISMS.	
7.	Procesy vztahů	
7.2.	Management vztahů s byznysem	částečně
	Chybí dokumentování schůzek, nabídek, poptávek a zakázek.	
7.3.	Management vztahů s dodavateli	ne
	Neřešeno z důvodu špatné vyjednávací pozice.	
8.	Procesy řešení	
8.2.	Management incidentů	ano
8.3.	Management problémů	ano
9.	Řídící procesy	
9.1.	Management konfigurací	částečně
	Problematika je řešena pouze povrchově. Není definováno co podléhá konfiguraci, jaké jsou objekty konfigurace a jejich atributy. Propojení databáze znalostí a databáze incidentů není plně automatizované. Databáze znalostí není plně uzpůsobena fungování jako CMDB.	
9.2.	Management změn	částečně
	Požadavky na změnu nejsou dostatečně dokumentovány a klasifikovány. Změny neobsahují informace o postupu pro vrácení do výchozího stavu. Nejsou analyzovány a vyhodnocovány trendy ohledně požadavků změn.	
10.	Proces uvolnění	
10.1.	Proces uvolnění	ano

Tabulka 5.2: Souhrnná tabulka zobrazující soulad s normou (zdroj vlastní).

6 PDCA

PDCA neboli Demingův cyklus, je metodou pro postupné zlepšování procesů. Důvodem začlenění této kapitoly do mé diplomové práce je, že normy ČNS ISO/IEC 27001:2006 (viz kaptiola 4 ISMS) a ISO/IEC 20000-1:2011 (viz kapitola 5 ITSM) jsou založeny na procesním přístupu řízení a Demingově cyklu.

6.1 Plánuj (Plan)

Většina obsahu této diplomové práce se zabývala tímto krokem. V práci jsem stanovil požadavky na procesy a následně jsem tyto procesy navrhl, včetně plánu zavádění a potřebného vybavení.

Cílem plánování bylo:

- identifikovat požadavky na řešení (viz 3.2 Požadavky na řešení),
- navrhnout pracovní pozice, jejich odpovědnosti a povinnosti (viz 3.3.1 Organizační struktura),
- identifikovat procesy (viz 3.3.2 Přehled procesů),
- navrhnout procesy (viz 3.3.4 Modely procesů),
- navrhnout informační systém (viz 3.4 Výběr vhodného softwaru),
- přizpůsobit navržené řešení managementu bezpečnosti informací (viz 4 ISMS),
- přizpůsobit navržené řešení managementu služeb (viz 5 ITSM).

6.2 Dělej (Do)

Z naplánovaných bodů již byly některé realizovány a zbytek bude realizován vlastními silami v období letních prázdnin roku 2012. Změny budeme zavádět nárazovou metodou zavádění (vše se připraví a pak se na řešení nárazově přejde).

6.3 Kontroluj (Check)

Zavedené řešení budeme průběžně vyhodnocovat na základě:

- spokojenosti zákazníků – dle pravidelných ročních setkání, konzultací s techniky, případných stížností zákazníků a počtu nových i ztracených zákazníků,
- dodržování smluvní úrovně služeb – měřené databází incidentů,
- kvality práce – počtu reklamací,
- bezpečnostních incidentů – dle databáze incidentů,
- spokojenosti zaměstnanců – dle pracovního nasazení a rozhovorů,
- finančních výsledků společnosti.

6.4 Jednej (Act)

Zjištěné nedostatky a možná vylepšení (dále jen jako „návrhy“) budou zaznamenávány do databáze znalostí. Na pracovních poradách budou tyto návrhy prodiskutovány a ohodnoceny z hlediska časové i finanční náročnosti a možného přínosu. Na základě ohodnocení bude rozhodnuto, kdy dojde k implementaci návrhu. Rozhodující slovo o implementaci návrhu bude mít jednatel společnosti.

Závěr

Tato práce se věnovala praktickému návrhu pracovních procesů pro moji společnost. Nejprve jsem společnost představil (viz kapitola 2 Profil společnosti), popsal její vývoj od historie až po budoucí představy a zaměřil jsem se také na marketingovou strategii společnosti.

Před samotným návrhem procesů (viz kapitola 3 Návrh procesů) jsem popsal jejich současný stav a identifikoval jsem požadavky na nové procesy. Navržené procesy jsem popsal slovně a vymodeloval pomocí BPMN. Vzhledem k tomu, že navržené procesy vyžadují podporu informačního systému, provedl jsem výběr vhodného softwaru pro informační systém, sestavil schéma možného nasazení a udělal kalkulaci nákladů na pořízení a provozování informačního systému.

Navržené procesy jsem vyhodnotil oproti normě „ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systém managementu bezpečnosti informací – Požadavky“ (viz kapitola 4 ISMS). Identifikoval jsem možné hrozby a zranitelnosti aktiv používaných v navržených procesech. Z normy jsem vybral vhodná opatření pro eliminaci zranitelností nebo snížení jejich dopadu a aplikoval je formou bezpečnostní politiky nebo bezpečnostních opatření. Na závěr jsem provedl kvantifikaci zbytkového rizika a výsledky okomentoval.

V kapitole 5 ITSM jsem zkoumal soulad navržených procesů oproti normě „ČSN ISO/IEC 20000-1:2006 Informační technologie - Management služeb“. Prošel jsem požadavky normy na navržené procesy a pro každý požadavek jsem určil, zda jsou s ním navržené procesy v souladu nebo nejsou.

V závěrečné kapitole 6 PDCA jsem se věnoval zejména nasazení navržených procesů, jejich monitorování a postupnému zlepšování.

Výsledkem mé práce jsou tedy navržené procesy, včetně organizační struktury a informačního systému. Tyto procesy byly vyhodnoceny oproti managementu služeb a managementu bezpečnosti informací. Dále byl pro tyto procesy popsán způsob zavádění a definovány ukazatele pro měření výkonosti.

Vše, co jsem v této práci navrhl a popsal, bude v druhé polovině roku 2012 převedeno do praxe a využito v mé společnosti PATRON-IT s.r.o.

Literatura

[1] SVOZILOVÁ, Alena. Zlepšování podnikových procesů. 1. vyd. Praha: Grada, 2011, 223 s. ISBN 9788024739380.

[2] VOSOBA, Pavel. Dokonalé služby: co chtějí zákazníci. 1. vyd. Praha: Grada, 2004, 164 s. ISBN 8024708477.

[3] DOUCEK, Petr et al. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 9788074310508.

[4] JANSA, Lukáš a Petr OTEVŘEL. Softwarové právo: praktický průvodce právní problematikou v IT. Vyd. 1. Brno: Computer Press, 2011, 340 s. ISBN 9788025134580.

http://www.omg.org/spec/BPMN/2.0/

[5] OBJECT MANAGEMENT GROUP, Inc. Business Process Model and Notation (BPMN) [online]. 2.0. 2011 [cit. 2012-05-05]. Dostupné z: http://www.omg.org/spec/BPMN/2.0/PDF/

[6] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 20000-1:2011. Information technology - Service management - Part 1: Service management system requirements. Geneva: International organization for Standardization 2011.

[7] ČESKÝ NORMALIZAČNÍ INSTITUT. ČSN ISO/IEC 20000-2:2007. Informační technologie - Management služeb - Část 2: Soubor postupů. Praha: Český normalizační institut 2007.

[8] ČESKÝ NORMALIZAČNÍ INSTITUT. ČSN ISO/IEC 27001:2006. Informační technologie - Bezpečnostní techniky - Systém managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut 2006.

[9] ČESKÝ NORMALIZAČNÍ INSTITUT. ČSN ISO/IEC 27002:2008. Informační technologie - Bezpečnostní techniky - Soubor postupů pro řízení bezpečnosti informací. Praha: Český normalizační institut 2008.

[10] ATSEC INFORMATION SECURITY CORPORATION. ISMS Implementation Guide [online]. 1.1. 2007 . Dostupné z: http://www.atsec.com/downloads/documents/ISMS-Implementation-Guide-and-Examples.pdf