VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

ÚSTAV SOUDNÍHO INŽENÝRSTVÍ

INSTITUTE OF FORENSIC ENGINEERING

POSOUZENÍ INFORMAČNÍHO SYSTÉMU U VYBRANÉ FIRMY A NÁVRH ZMĚN

INFORMATION SYSTEM ASSESSMENT AND PROPOSAL FOR ICT MODIFICATION

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Ing. David Manda**
AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. Miloš Koch, CSc.**
SUPERVISOR

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
ÚSTAV SOUDNÍHO INŽENÝRSTVÍ

Zadání diplomové práce

Ústav:	Ústav soudního inženýrství
Student:	**Ing. David Manda**
Studijní program:	Rizikové inženýrství
Studijní obor:	Řízení rizik v informačních systémech
Vedoucí práce:	**doc. Ing. Miloš Koch, CSc.**
Akademický rok:	2016/17

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma diplomové práce:

Posouzení informačního systému u vybrané firmy a návrh změn

Stručná charakteristika problematiky úkolu:

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

Cíle diplomové práce:

Analyzovat stávající stav informačního systému vybrané organizace a jeho efektivnosti, posoudit tento stav a navrhnout změny, směřující ke zlepšení stávajícího stavu a eliminaci nalezených rizik.

Seznam doporučené literatury:

BASL, Josef; BLAŽÍČEK, Roman. Podnikové informační systémy: Podnik v informační společnosti. 2. výrazně přepracované a rozšířené vydání. Praha : Grada Publishing, 2000. 283 s. ISBN 978-80-2-7-2279-5.

DOSTÁL, Petr; RAIS, Karel; SOJKA, Zdeněk. Pokročilé metody manažerského rozhodování. 1. vydání. Praha : Grada Publishing, 2005. 168 s. ISBN 80-247-1338-1.

MOLNÁR, Zdeněk. Efektivnost informačních systémů. 1. vydání. Praha : Grada Publishing, 2000. 144 s. ISBN 80-7169-410-X.

ŘEPA, Václav. Podnikové procesy : Procesní řízení a modelování. 2. aktualizované a rozšířené vydání. Praha : Grada Publishing, 2007. 288 s. ISBN 978-80-247-2252-8.

SODOMKA, Petr. Informační systémy v podnikové praxi. 1. vydání. Brno : Computer Press, a.s., 2006. 351 s. ISBN 80-251-1200-4.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2016/17

V Brně, dne

L. S.

.....

doc. Ing. Aleš Vémola, Ph.D.
ředitel

Abstrakt (vzor)

Tato diplomová práce je zaměřena na problematiku informačních systémů ve firmách. Cílem práce je navrhnout změny v informačním systému organizace na základě analýz. Práce obsahuje ekonomické zhodnocení při realizaci změn.

Abstract

This master thesis is focused on issues in the field of information systems in companies. The purpose of this thesis is to propose changes in the information system of the organization based on analyzes. The thesis includes economic evaluation for the implementation of modification changes.

Klíčová slova

informační systém, analýza, HOS 8, Zefis

Keywords

information system, analysis, HOS 8, Zefis

Bibliografická citace

MANDA, David. *Posouzení informačního systému u vybrané firmy a návrh změn*. Brno, 2017. 58 s. Vysoké učení technické v Brně, Ústav soudního inženýrství. Vedoucí diplomové práce Ing. Miloš Koch, CSc.

Prohlášení

Prohlašuji, že jsem diplomovou práci zpracoval/a samostatně a že jsem uvedl/a všechny použité informační zdroje.

V Brně dne ……..

…….

podpis diplomanta

Poděkování

Na tomto místě bych rád poděkoval doc. Ing. Miloši Kochovi, CSc., vedoucímu této diplomové práce, za umožnění vytvořit tuto diplomovou práci a za poskytnutí systému Zefis.

Obsah

1 ÚVOD

V dnešní době jsou informační systémy nedílnou součástí současného světa. Již dávno nejsou pouze doménou velkých a středních firem, nyní se stávají nutností pro skoro každou menší firmu nebo i pro samostatného živnostníka. Kvalitní informační systém a jeho úspěšné zavedení ve firmě může vést ke zlepšení efektivity práce, úspoře nákladů a k celkovému zvýšení ziskovosti společnosti.

Výběr a následná implementace informačního systému je poměrně složitý proces. V mnoha případech to stojí spoustu úsilí a peněz, a proto je důležité těmto činnostem věnovat maximální pozornost. Mají totiž zásadní vliv na to, jestli informační systém firmě nakonec něco přinese či nikoliv.

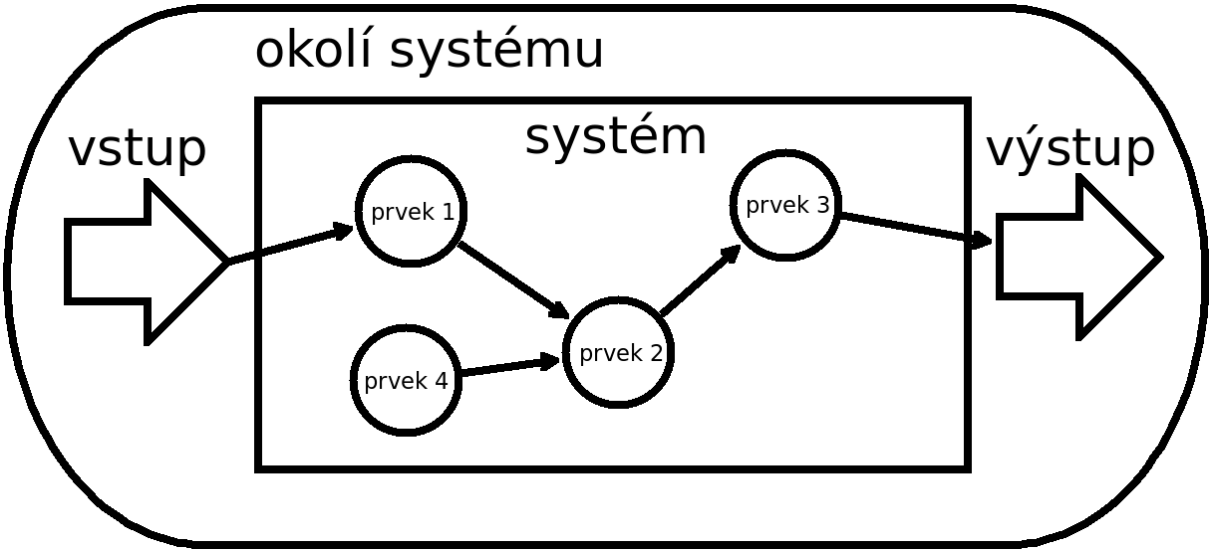
Hlavním cílem diplomové práce je analyzovat stávající stav informačního systému vybrané organizace a jeho efektivnosti, posoudit tento stav a navrhnout změny směřující ke zlepšení stávajícího stavu.

2 CÍL PRÁCE

Cílem této diplomové práce je analyzovat stávající stav informačního systému vybrané organizace a jeho efektivnosti, posoudit tento stav a navrhnout změny směřující ke zlepšení stávajícího stavu a eliminaci nalezených rizik. Pro tuto práci byla vybrána marketingová a internetová agentura z Brna, která zde bude vystupovat pod fiktivním názvem XY, jelikož si přeje kvůli interním důvodům zůstat v anonymitě.

3 TEORIE SYSTÉMŮ

Teorie systémů je obor zabývající se zkoumáním systémů z metodologického aspektu. S využitím teorie systémů se můžeme setkat v mnoha oborech, od informatiky, přes fyziku až k filozofii. Podle Molnára je systém definován jako uspořádaná množina prvků, která spolu s jejich vlastnostmi a vztahy mezi nimi vykazuje jako celek určité vlastnosti, tzv. chování. Obecně tedy lze systém charakterizovat jako celek složený z částí, které na sebe navzájem působí. [2] Na obrázku 1 je zobrazen vzorový příklad systému.



Obr. 1 Systém (vlastní tvorba)

Základní atributy systému:

- Okolí systému – jedná se o takovou entitu, která je zdrojem podnětů působících na systém a která přijímá reakce systému na tyto podněty
- Vstup systému – množina vazeb či proměnných, jejichž prostřednictvím získává systém informace ze svého okolí
- Výstup systému – množina vazeb či proměnných, pomocí kterých systém předává informace do svého okolí
- Prvek systému – jsou dále nedělitelné (elementární) části systému, které představují jeho dekompoziční části. Pomocí těchto prvků jsou charakterizovány strukturální vlastnosti systému

- Vazba systému – zajišťuje spojení mezi jednotlivými prvky systému.

3.1 SYSTÉMOVÝ PŘÍSTUP

Systémový přístup vychází z teorie systémů. Je to účelový způsob myšlení, či řešení problémů, přičemž zkoumané jevy a procesy jsou chápány komplexně (celistvě) v jejich vnitřních a vnějších souvislostech. Obecně lze systémový přístup charakterizovat jako „nápovědu“, na jaké podstatné skutečnosti by neměl člověk ve svém jednání, myšlení a ve veškerých svých činnostech zapomenout a jakým způsobem by měl optimálně tyto činnosti realizovat. Janíček ve své publikaci popisuje těchto 21 atributů systémového přístupu: [3]

0. Systémový přístup je zobecněnou metodologií vědeckého a praktického poznávání.

1. Požadavek pojmové čistoty – je charakterizována významově a obsahově správným vymezením pojmů.

2. Správné vymezení a formulace problémů.

3. Entity posuzovat strukturovaně – strukturovanost znamená, že na entitě lze vymezit další prvek, který má charakter entity vyšší úrovně.

4. Entity posuzovat účelově – důležité je posuzovat podstatnost.

5. Entity posuzovat komplexně – komplexnost znamená analyzovat entitu ve všech vnitřních a vnějších souvislostech.

6. Entity posuzovat hierarchicky – hierarchie vyjadřuje stupňovitou soustavu hodnot určité entity.

7. Entity posuzovat orientovaně – rozlišujeme časovou, příčinnou a hierarchickou orientovanost.

8. Posuzovat otevřenost entity – podle otevřenosti rozlišujeme, jaké interakce má entita se svým okolím.

9. Posuzovat úrovňovou vyváženost

10. Posuzovat dynamičnost entity – entity jsou zkoumány v závislosti na čase

11. Posuzovat stochastičnost entity

12. Posuzovat cílené chování entit – pod pojmem cílené chování se rozumí to, co má být ideálně dosaženo.

13. Posuzovat entity z hlediska výskytu deterministického chaosu a z hlediska výskytu samoorganizace

14. Využívat poznatky současné vědy a techniky

15. Pří řešení nestandardních situací používat progresivní a heuristické metody

16. Vytvářet algoritmy činností – posloupnost činností, které vedou ke splnění určitého cíle.

17. Analyzovat výsledky řešení problémů (z hlediska jejich důvěryhodnosti)

18. Řešitel problému má zodpovědnost za věrohodnost předávaných výsledků

19. Dodržovat veškeré etické normy

20. Sledovat způsob implementace výsledků

3.2 SYSTÉMOVÉ MYŠLENÍ

Myšlení je nejvyšší formou psychického procesu odehrávající se v lidském mozku. Pod pojmem systémové myšlení se rozumí myšlení v atributech systémového přístupu. V oblasti psychologie se vymezují zejména tyto typy myšlení: [3]

- Produktivní myšlení – cílevědomé myšlení něco vytvořit. Protipólem je reproduktivní myšlení (přijímání cizího stylu myšlení).
- Analyticko-syntetické myšlení – schopnost dekomponovat zkoumané entity na prvky a na těchto prvcích řešit problémy.
- Reaktivní myšlení – protipól je spontánní myšlení.
- Divergentní myšlení – myšlení víceznačné. Protipólem je konvergentní myšlení.
- Tvůrčí (kreativní) myšlení – schopnost vytvořit něco originálního. Protipól je myšlení konvenční.

Komplexní myšlení – shrnuje všechny předcházející typy a je vrcholem myšlení.

3.3 KLASIFIKACE SYSTÉMŮ

Systémy můžeme dělit podle následujících kritérií: [3]

- uzavřené x otevřené – dělí se podle toho, zda nastává nebo nenastává interakce s okolím.
- deterministické x nedeterministické (stochastické) - zatímco u deterministických systémů je způsob chování jednoznačně určen dopředu, u stochastických se předpokládá více variant chování.
- dynamické x statické – dělení podle toho, zda se vyvíjejí v čase.
- informační systémy – jsou to systémy, u kterých vazby představují informace a prvky jsou místem transformace těchto informací.

4 INFORMAČNÍ SYSTÉMY

Existuje spousta různých definic informačního systému. Molnár definuje informační systém jako systém, který je souborem lidí, technických prostředků a metod, zabezpečující sběr, přenos, zpracování a uchovávání dat s cílem prezentace informací pro potřeby uživatelů činných v systémech řízení. [4]

4.1 ZÁKLADNÍ POJMY

Níže je přehled základních pojmů v oblasti informačních systémů.

4.1.1 Data

Data můžeme chápat jako vstupy do datového modelování, jehož výstupem jsou informace. Jsou nezávislá na uživateli, většinou odráží současný stav reality a poměrně často a rychle se mění. Data vždy zjednodušují komplexnost reality (jsou nekompletní). [4]

4.1.2 Informace

Za informace se dají považovat data, která mají nějaký význam (sémantiku). Informace z dat vytváří uživatel jejich interpretací. Jedná se tedy o subjektivní proces, který může každý z uživatelů provádět jiným způsobem, a tím mohou vznikat různé problémy. Vlastnosti kvalitní informace jsou následující: [4]

- přesnost – je jasná a neobsahuje chyby
- včasná – je k dispozici ve vhodném čase
- relevantní
- srozumitelná

Informace nevznikají najednou, ale průběžně.

4.1.3 Znalosti

Data, znalosti a informace spolu úzce souvisí. Podle Beckmanovy teorie je znalost definována jako uvažování nad daty a informacemi za účelem aktivního výkonu, řešení problému, rozhodování, učení a výuky. Znalost jedinec získá po osvojení si informací a jejich začlenění do souvislostí. [5]

4.1.4 Informační technologie

Obvykle chápeme jako souhrn všech technických (hardware), programových (software), telekomunikačních, organizačních a dalších prostředků, technik a služeb, které je možno využívat při jednotlivých operacích s informacemi.

4.1.5 Firma

Firma je produkční jednotka, která vykonává podnikatelské aktivity s cílem realizovat zisk. Obvykle se výraz „firma“ používá i jako synonymum slova podnik. Mezi další cíle vedle maximalizace zisku patří např. dlouhodobé přežití na trhu, růst, expanze do dalších oblastí atd.

4.2 KOMPONENTY INFORMAČNÍHO SYSTÉMU

Informační systém se skládá z následujících komponent: [6]

Hardware – jedná se o všechny technické prostředky. Patří tam počítače (osobní počítače, servery) a jejich bezprostřední komponenty (operační paměti, procesory), periferní zařízení (tiskárny, různé snímače), síťové komunikační prostředky (kabeláž, odbočovače), provozní materiál (papír do tiskáren, optické disky) atd.

Software – označení pro programové vybavení počítačů. Jedná se o nehmotné počítačové vybavení.

Orgware – jedná se o organizační prostředky. Obecně chápeme jako soubor nařízení a pravidel definující provoz a využívání informačního systému a informačních technologií.

Peopleware – lidská složka informačního systému. Tato složka zahrnuje uživatele včetně jejich znalostí a chování ve vztahu k informačnímu systému.

Reálný svět – informační zdroje, legislativa, normy.

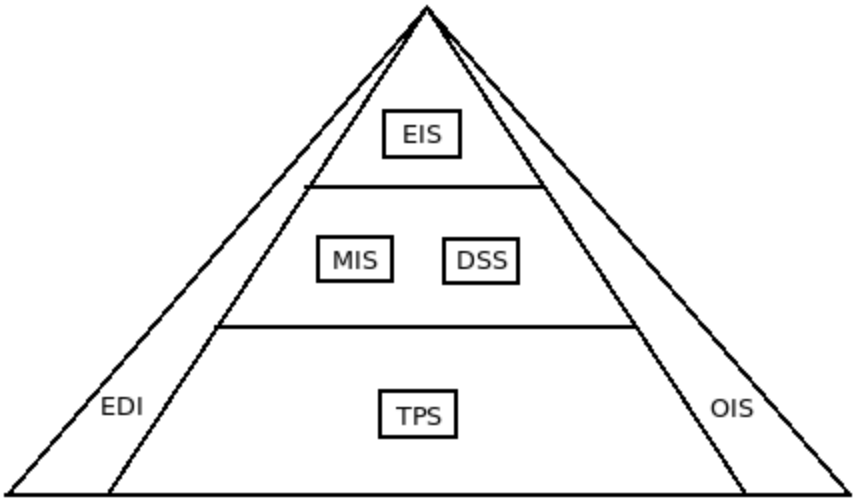
4.3 ARCHITEKTURA INFORMAČNÍHO SYSTÉMU

Architektura informačního systému je vyjádření celkové koncepce informačního systému. Architektura vytváří poměrně stabilní rámec pro řízení tvorby informačního systému, do něhož jsou postupně začleňovány jednotlivé technologické a programové součásti v závislosti na potřebách a podmínkách podniku.

V průběhu fungování informačního systému se architektura (při zachování její koncepce) obvykle neustále upravuje a přizpůsobuje měnícím se požadavkům. [6]

4.3.1 Globální architektura

Globální architektura je složena z dílčích stavebních bloků a je považována za základní architekturu informačního systému. Blok je množina informačních služeb a funkcí, které slouží k podpoře podnikových procesů (jednoho nebo více). Globální architekturu ve formě informační pyramidy zachycuje obrázek 2.



Obr. 2 Globální architektura (vlastní tvorba)

***EIS* (*Executive Information Systems*) –** jsou to řídící informační systémy, které zabezpečují vrchol řídící pyramidy, jsou určeny pro strategické řízení podniku. Využívají všech dostupných informačních zdrojů, které jsou vytvářeny na nejnižších úrovních informačního systému. Modely *EIS* mohou být obvykle naplňovány čtyřmi způsoby: [6]

- vlastním vstupem uživatelů (zřídka).
- konverzí z původních databází ze systémů nižších úrovní.
- konverzí z jiných systémů *EIS* (od konkurence, z jiných poboček atd.).
- konverzí z externích databází.

MIS (*Management Information Systems*) – manažerský informační systém**,** je určen pro řízení podniku na taktické úrovni. Data do tohoto systému se získávají z transakčních systémů obvykle v agregované formě. [6]

DSS (*Decision Support Systems*) – určen pro manažerské plánování všeho druhu (pro úroveň operativního i taktického řízení). Vstupními daty bývají většinou data z manažerských informačních systémů. [6]

TPS (*Transaction Processing Systems*) – jedná se o provozní nebo také transakční informační systémy, se kterými pracují především zaměstnanci na operativní úrovni řízení. Je robustní, spolehlivý a s rychlou odezvou. Existují různé typy TPS, jako např.: [6]

- CRM (Customer Relationship Management) – zákaznicky orientovaný management, zabývá se aktivní tvorbou a udržováním dlouhodobě prospěšných vztahů se zákazníky. Umožňuje pochopit a předvídat potřeby, přání a nákupní zvyklosti zákazníků, a podporuje oboustrannou komunikaci mezi firmou a jejími zákazníky.
- ERP (Enterprise Resource Planning) – jde o podnikový informační systém, integruje všechny nebo většinu oblastí své činnosti, jako jsou plánování, zásoby, nákup, prodej, finance, marketing atd. [1]
- GIS (Geographic Information System) – geografický informační systém, umožňuje sběr a správu prostorových dat neboli geodat, poskytuje nástroje pro jejich analýzu a pro grafickou prezentaci výsledných prostorových modelů zájmového území.
- CAM (Computer Aided Manufacture) - automatizovaná podpora řízení výrobních procesů.

EDI (*Electronic Data Interchange*) – jedná se o způsob výměny strukturovaných dat na základě dohodnutých standardů mezi informačními systémy jednotlivých obchodních partnerů pomocí elektronických prostředků. [6]

OIS (*Office Information System*) – slouží k podpoře rutinní kancelářské práce, zvyšuje produktivitu a výkonnost administrativních pracovníků. [6]

4.3.2 Dílčí architektury

Z globální architektury se odvozují následující dílčí architektury: [6]

Procesní architektura – cílem této architektury je co nejrychlejší reakce podniku na externí události při nízké spotřebě podnikových zdrojů. Tyto klíčové externí události představují podstatné vazby podniku s okolím. Nástrojem na zachycení těchto vazeb se používá kontextový diagram.

Funkční architektura – navazuje na procesní architekturu, je návrhem hierarchického rozpadu požadovaných funkcí a služeb informačního systému. Funkce v hierarchii představují statický pohled na informační systém.

Datová architektura – je návrhem datové základny informačního systému. Hojně používaný datový model pro tvorbu databáze je relační model.

Softwarová architektura – určuje programy a komponenty, ze kterých se informační systém bude skládat. Součástí této architektury jsou i vazby mezi jednotlivými programy.

Hardwarová architektura – určuje typy, počty a vzájemné vazby hardware komponent (serverů, osobních počítačů, tiskáren), a dalších přídavných zařízení.

Technologická architektura – rozhoduje o technologickém řešení aplikace. Navazuje na technickou, datovou a programovou architekturu. Definuje způsob zpracování jednotlivých aplikací.

4.4 BEZPEČNOST INFORMAČNÍCH SYSTÉMŮ

Pod pojmem počítačová bezpečnost si můžeme představit ochranu počítačových prostředků proti náhodnému nebo úmyslnému prozrazení důvěrných dat, neoprávněné modifikaci dat nebo programů, zničení dat, software nebo hardware, a neoprávněnému zabránění v použití počítačových prostředků. S tím, jak se informační systémy stále více stávají nedílnou součástí firem a organizací, narůstají útoky a potenciální škody, které mohou být způsobeny kyberzločinci, zloději nebo malwarem. [7]

Cíle bezpečnosti informačních systémů jsou následující: [7]

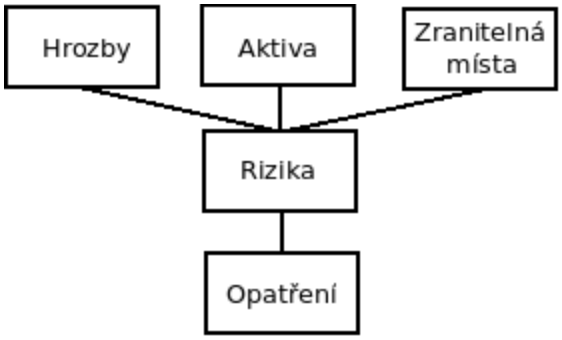
- důvěrnost (confidentiality) – jde o ochranu proti neoprávněnému prozrazení informace. Může být porušena např. prolomením slabého hesla, rozluštěním šifrovaných zpráv nebo nevhodně přidělenými právy. Důvěrnost lze zabezpečit pomocí šifrování, skrýváním identit počítačů organizace za firewally atd.
- integrita (integrity) – integrita by měla zajišťovat ochranu proti neoprávněné modifikaci informace. Pro zajištění integrity dat lze použít elektronického podpisu a certifikátů na bázi asymetrické kryptografie nebo mechanismů kryptografických kontrolních součtů.
- dostupnost (availability) – jedná se o ochranu proti neoprávněnému odepření přístupu k datům nebo ke službám. Toto opatření se realizuje např. omezením délek elektronicky vyměňovaných zpráv. Typickým útokem způsobující ohrožení dostupnosti je útok typu Denial of Service.
- autentičnost (authentication) – jedná se o požadavek na zaručení ověřitelnosti původu informace. Komunikující strany musí mít jistotu, že komunikují s tím partnerem, se kterým komunikovat chtěly. To může být zajištěno např. elektronickým podpisem.

4.4.1 Útočníci

Útočníci mohou úspěšně provádět své útoky jak uvnitř organizace (vnitřní útočník), tak i z vnějšího okolí (vnější útočník). Útočníky obvykle dělíme podle jejich znalostí, prostředků (vybavení a čas) a příležitostí. Využívají zranitelných míst, což jsou slabiny v informačním systému, která mohou být využita pro provedení bezpečnostního incidentu (útoku).

Těchto zranitelných míst využívají hrozby, což jsou okolnosti, které mají potenciál způsobit bezpečnostní incident, a ohrozit tak aktiva firmy. Hrozby mohou být různé, např. fyzický útok, krádež hesla nebo malware a jiné nepřátelské programy. Do hrozeb patří i útočníci. V kombinací se zranitelnými místy pak vytvářejí riziko.

Na hrozby a rizika se reaguje různými opatřeními, které mají potenciál redukovat pravděpodobnost vzniku bezpečnostního incidentu. Existují opatření dvojího druhu, a to opatření preventivní, a opatření omezující (minimalizuje ztráty a maximalizuje zotavení po útoku). U opatření je vždy potřeba zvážit jejich efektivitu – náklady na opatření by neměla být vyšší než předpokládaná ztráta způsobená útokem.



Obr. 3 Vztahy mezi pojmy bezpečnosti IS (vlastní tvorba)

V informační bezpečnosti rozlišujeme tři typy útočníků: [7]

- útočník slabé síly – jde především o náhodné útočníky využívající náhodně objevená zranitelná místa při své běžné práci. Tito útočníci mají omezené znalosti, prostředky i příležitosti, je možné proti nim přijmout i relativně slabá bezpečnostní opatření.
- útočník střední síly – největší motivací těchto útočníků je dostat se k tomu, k čemu nejsou autorizovaní. Jde především o hackery, kteří sice mají hodně znalostí, ale obvykle disponují omezenými prostředky, a také nemají tolik příležitostí k útoku.
- útočník velké síly – tyto typy útočníků jsou ze všech nejnebezpečnější, protože jsou typičtí vysokou úrovní svých znalostí, a taktéž mají dostatek prostředků. Jsou to hodně často počítačoví experti, kteří provádějí útoky vymykající se běžné praxi. Tyto útočníky mohou zastavit pouze ta nejsilnější bezpečnostní opatření.

4.4.2 Malware

Malware je termín používaný k označení škodlivého softwaru, který je navržen tak, aby poškodil počítačový systém nebo v něm prováděl takové akce, ke kterým nemá potřebná oprávnění.

Viry – jedná se počítačový program, který se schopen šířit se pomocí replikace (tedy vytváří kopie sebe sama). Provádí to tak, že do jiného programu zkopíruje své tělo, čímž se infikovaný program stane prostředkem pro další aktivaci viru. Pro své šíření tedy potřebuje nějakého hostitele. Tímto hostitelem můžou být například systémové oblasti disku nebo spustitelné soubory. Jestliže virus infikuje počítač s operačním systémem Windows, může napadnout registr, nahradit systémové soubory nebo převzít kontrolu nad programy pro elektronickou poštu. Velká většina virů je naprogramována v jazyce symbolických adres. Viry je možno dělit do několika kategorií : [8]

- boot sector viry – napadají systémové oblasti pevného disku, spuštění si vir zajistí ihned se startem počítače. Tento typ viru patří mezi nejstarší.
- souborový infektor – napadají spustitelné soubory operačního systému. Jedná se o soubory přímo spustitelné (com, exe), dávkové soubory (bat), binární soubory (bin) nebo systémové soubory (sys).
- makroviry – tento typ viru se zaměřuje na dokumenty. Využívá toho, že tyto dokumenty neobsahují pouze data, ale i makra, které využívá ke svému šíření. Jsou napadány především dokumenty aplikací MS Office.
- multipartitní viry – tento druh vznikl sloučením bootovacích virů a souborových infektorů. Je tedy schopen infikovat jak zaváděcí sektor pevného disku, tak i spustitelný program.

Červi – červi jsou na rozdíl od virů nezávislé programy, které se replikují tak, že se samy kopírují z jednoho počítače na druhý. Nepotřebují tedy žádný hostitelský program. Nejčastěji se mohou šířit přes počítačovou síť nebo prostřednictvím příloh elektronické pošty. Může zapříčinit zničení datových souborů nebo způsobovat útoky na jiné počítače. Často má

za cíl také vytvářet backdoor (tzv. zadní vrátka), který útočníkům umožní přístup do systému. [8]

Trojské koně – trojský kůň je škodlivý program, který provádí nějakou skrytou činnost bez vědomí nebo souhlasu napadeného. Většina trojských koňů vykonává činnosti, které můžou narušit zabezpečení počítače pomocí krádeží hesel, mazáním souborů nebo připojováním přes síť k jiným počítačům. Trojský kůň není na rozdíl od virů schopen replikace, nenapadá soubory a ani není připojen k žádnému hostiteli. Mezi trojské koně patří i tzv. *keyloggery*, tedy aplikace zaznamenávající uživatelem stisknuté klávesy. Všechny stisknuté klávesy se ukládají do určeného souboru a poté se mohou rovnou posílat k útočníkovi. [8]

Rootkity – za rootkit je považován takový softwarový balík, které je určen k tomu, aby vytvořil, utajil a spravoval prostředí pro útočníka na napadeném stroji. Má schopnosti maskovat přítomnost nebezpečného software (virů, trojských koňů), dokonce ho útočník může použít k eliminaci důkazů (odstranění důkazu o útoku a zabránění vzniku nového důkazu). V současnosti existují tři druhy rootkitů : [8]

- binární rootkity – útočníci je zpravidla používají k nahrazení důležitých systémových souborů. Tím lze dosáhnout několika cílů, například si útočník dokáže zajistit vzdálený přístup, lokální přístup nebo ukrytí důkazů.
- kernelové rootkity – dokáží měnit jádro operačního systému. Mají za úkol zaměřovat se především na změnu důležitých systémových volání (syscalls) pomocí připojení na kernelové moduly LKM (Loadable Kernel Module).
- rootkity přepisující systémové knihovny.

4.5 ŽIVOTNÍ CYKLUS INFORMAČNÍHO SYSTÉMU

Životní cyklus informačního systému můžeme rozčlenit na následující části: [1]

specifikace problému – cílem je posoudit realizovatelnost projektu

a**nalýza –** logický model, popisuje podrobnějším způsobem požadavky na informační systém z předchozí etapy.

návrh – technologický model, po této fázi by mělo být možné systém implementovat. Dochází i k návrhu uživatelského rozhraní.

implementace – realizace detailního návrhu v implementačním prostředí, včetně testování. V této fázi se taktéž vyhotovuje programová dokumentace a někdy i uživatelská příručka.

zavádění – v této fázi se prování instalace programového a technického vybavení, vytvoření provozních pokynů a zaškolení uživatelů.

provoz a údržba – cílem je zajistit bezproblémový provoz a údržbu nejen informačního systému, ale také aktualizace dokumentace a realizace změn.

4.6 TECHNOLOGIE PŘI IMPLEMENTACI

V této podkapitole jsou popsány technologie, které se hojně využívají při implementaci informačních systémů.

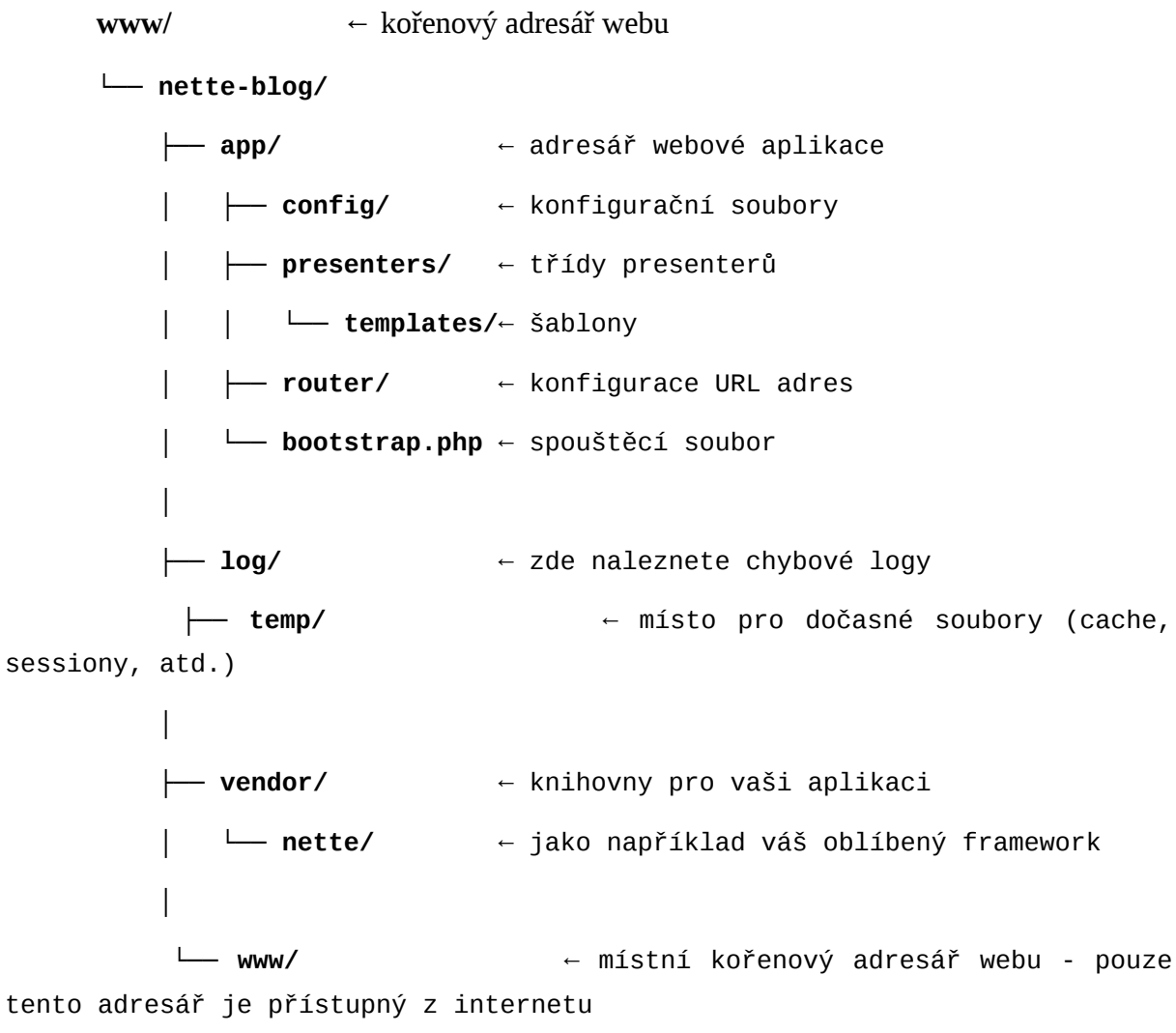
4.6.1 PHP

PHP je skriptovací programovací jazyk určený především pro programování dynamických internetových stránek a webových aplikací například ve formátu *HTML* nebo *XHTML*. Při použití *PHP* pro dynamické stránky jsou skripty prováděny na straně serveru, a k uživateli je přenášen až výsledek jejich činnosti [10]. V současnosti se nachází ve verzi 7.1.

4.6.2 Nette Framework

Nette Framework je v současnosti nejpoužívanějším frameworkem v České republice. Jedním z důvodu může být i to, že velké množství dokumentace a oficiální fórum je psané v českém jazyce. Framework je v podstatě souhrn funkcí (metod), které programátor využívá pro práci.

Frameworky obvykle dodržují nějakou základní architekturu. V případě Nette frameworku se jedná o MVC architekturu, jejíž zkratka (M – model, V – view, C - controller) určuje jednotlivé komponenty, ze kterých je framework postavený. Tento návrhový vzor získal popularitu hlavně ve webových aplikacích, ale jeho původ pochází z desktopových aplikací.



Obr. 4 Adresářová struktura Nette Frameworku [11]

Základní myšlenkou MVC architektury je oddělení logiky od výstupu. Před tímto způsobem řešení se často ve webových aplikacích míchaly logické operace (např. databázové dotazy) s jazykem HTML, což značně znepřehledňovalo zdrojový kód. Tento problém řeší právě MVC architektura, která rozděluje aplikaci na tři komponenty:

model – model obsahuje logiku aplikace. Nemá vůbec žádné informace, odkud přicházejí jednotlivé parametry, anebo jakým způsobem je řešený výstup dat. Může se starat o různé logické výpočty, databázové dotazy atd.

view – jak už název napovídá, view se stará o zobrazení výstupu. Podobně jako model nic neví o původu dat a obsahuje pouze základní logiku, jakým způsobem se data mají

zobrazit. Jedná se v podstatě o HTML šablonu, která zpracovává data, a následně je vykresluje

controller – slouží k propojení modelu se šablonou (view). Controller komunikuje s modelem a view drží celý systém pohromadě.

V případě Nette Frameworku je model základem celé aplikace, který poskytuje pevně dané rozhraní. Není určené, jakým způsobem má uživatel pracovat s databázemi. Nette samotné nabízí vlastní řešení v podobě Nette Database, ale existuje více možností práce s databází, např. se může využít ORM (objektově relační mapování pomocí Doctrine 2).

Nette aplikace komunikuje přes soubor *index.php*, který se nachází ve složce *www/*. Tento soubor posouvá řízení dále do aplikace, a to do souboru *bootstrap.php*, který se stará o zavedení všech potřebných souborů pro běh aplikace.

5 ANALÝZA PROBLÉMU

Tato kapitola práce má za úlohu představení společnosti, analyzovat současný stav situace a přestavit informační systém, který se ve firmě používá. V rámci kapitoly je taktéž vyhodnocení metodou HOS 8. Analýzy, které tvoří velkou část této kapitoly, byly získány z dat, informací a poznatků z rozhovorů s jednatelem společnosti a s jeho zaměstnanci.

5.1 PŘEDSTAVENÍ SPOLEČNOSTI

Pro tuto práci byla vybrána firma, která zde bude vystupovat pod fiktivním názvem XY, jelikož si přeje kvůli interním důvodům zůstat v anonymitě. Firma byla založena v roce 2010 a sídlo má momentálně v Brně Žabovřeskách, a jedná se o internetovou a marketingovou agenturu. Hlavní činnosti firmy se dají rozdělit do třech kategorií – vývoj webových aplikací, internetový (výkonnostní) marketing a reklamní design. Firma má momentálně 10 zaměstnanců.

Podrobnější popis činností:

vývoj webových aplikací*:*

- webové stránky a aplikace
- mobilní aplikace
- e-shopy

internetový marketing*:*

- PPC kampaně
- komunikační strategie
- webová analytika

reklamní design*:*

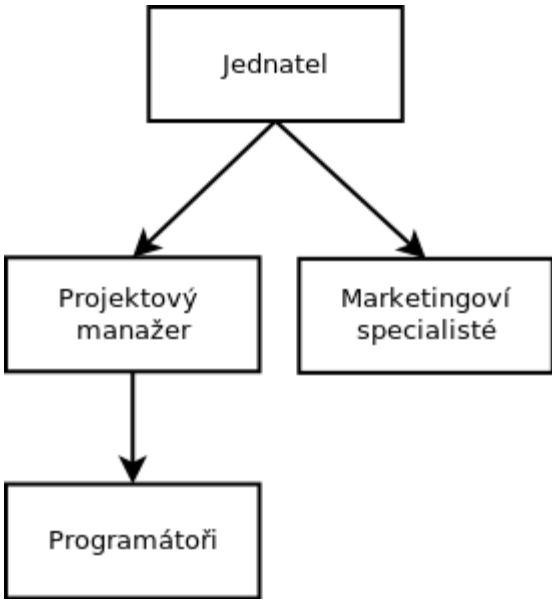
- grafické návrhy
- tvorba log

5.2 ANALÝZA 7S

Tato metoda je určena pro hodnocení kritických faktorů společnosti představujících nutnou podmínku pro úspěch libovolné organizace při realizaci její podnikové strategie. Těchto faktorů je celkem sedm a všechny začínají na písmeno „S“. Jsou to faktory strategie, struktura, spolupracovníci, styl, systémy, schopnosti a sdílené hodnoty. [9]

5.2.1 Struktura

Na vrcholu organizační struktury se nachází jednatel (zakladatel) společnosti. Pod jednatelem se nachází projektový manažer, který má na starosti tým vývojářů, a dva marketingoví specialisté (viz. obr. 5 níže). Komunikace mezi zaměstnanci probíhá většinou ústní nebo elektronickou formou, jen výjimečně telefonickou formou. Projektový manažer se společně s programátory stará především o vývoj webových aplikací, marketingoví specialisté zase zodpovídají za internetový marketing. Na jednateli společnosti je získávání nových zakázek a hlavní komunikace s klienty.



Obr. 5 Struktura ve firmě (vlastní tvorba)

5.2.2 Strategie

V porovnání s jinými firmami má společnost XY netradiční přístup ke strategii a filozofii společnosti. Samozřejmě má stejně jako ostatní společnosti jako hlavní cíl dlouhodobější růst a být spolehlivým a dobrým partnerem pro všechny. Mimo to klade důraz i na tom, aby společnost pracovala pouze pro ty klienty, se kterými má stejný pohled na business.

Firma si zakládá na dobrých referencích a odmítá takové zakázky, které by mohly poškodit její reputaci (např. byla odmítnuta zakázka na webovou stránku poskytující nevýhodné půjčky). Dá se říct, že společnost si své zákazníky vybírá.

5.2.3 Systémy

Zaměstnanci společnosti používají ke své práci vlastní interní informační systém. Tento systém byl navržen, implementován a testován pracovníky firmy, a je možné ho dále vyvíjet. Do systému mají kromě zaměstnanců firmy přístup taktéž zákazníci, kteří zde mohou přímo zakládat úkoly.

Implementace systému je provedena v Nette Frameworku ve verzi 2.3, a ve skriptovacím jazyce PHP ve verzi 5.6. Informační systém je hostován u společnosti WEDOS Hosting. Zde má firma hostovány i své webové stránky. Podrobnějšímu popisu systému je věnována podkapitola 5.3.

5.2.4 Styl

Zaměstnanci mohli vyjadřovat své názory nebo i výtky demokratickým způsobem, a to buď projektovému manažerovi (v případě vývojářů), nebo i přímo majiteli společnosti. Bohužel tohle v poslední době už moc neplatí. Pokud se vyskytnou nějaké vážnější problémy, jsou s dotyčným projednány s majitelem vždy pouze soukromě, nikdy ne před kolegy.

5.2.5 Spolupracovníci

Ve firmě zaměstnanci tvoří dobrý pracovní kolektiv, a vetšinou panuje přátelská nálada. Všichni zaměstnanci včetně majitele nemá více jak 30 let. Spolupracovníci spolu normálně komunikují a v případě problémů jsou si schopni poradit. Zaměstnanci jsou loajální

vůči svým nadřízeným.

5.2.6 Sdílené hodnoty

Společnost XY si zakládá na slušném jednání se zákazníky a na rychlosti vyřízení jejich požadavků. Firmu zajímá úspěch jejich klientů a chce jim vždycky přinést nějakou přidanou hodnotu. V neposlední řadě je důležitá kvalita a přesnost odvedené práce.

5.2.7 Schopnosti

Většina zaměstnanců má vysokoškolské vzdělání v oboru (IT nebo marketing). V svém volném čase se musí dále vzdělávat a sledovat nové trendy ve svém oboru.

5.3 POPIS INFORMAČNÍHO SYSTÉMU

Tato podkapitola popisuje aktuální stav informačního systému používaný ve společnosti. Jak už bylo zmíněno v podkapitole výše, informační systém byl vytvořen programátory, kteří jsou v současnosti zaměstnanci firmy. Vytvářen byl přibližně tři měsíce převážně jedním programátorem, další programátor prováděl testování systému, a částečně se také spolupodílel na implementaci. Implementace systému je provedena v Nette Frameworku ve verzi 2.3, a ve skriptovacím jazyce PHP ve verzi 5.6. Jako databázový systém je zvolen MySQL, verze 5.6.

Přihlášení do systému probíhá pomocí uživatelského jména a hesla. K autentizaci slouží třída *UserAuthenticator*, která implementuje rozhraní *Nette\Security\IAuthenticator* mající jedinou metodu *authenticate(array $credentials)*, která má jako parametr pole obsahující uživatelské jméno a heslo, tedy to, co uživatel vyplní při přihlašování. Třída *UserAuthenticator* komunikuje s databází a pracuje s tabulkou *users*, ve které je sloupec *username* (uživatelské jméno) a *password* (heslo uživatele). Funkce *authenticate* buď vrátí identitu uživatele (pokud uživatel existuje a je zadáno správné heslo), nebo vyhodí výjimku s chybovou hláškou, a přihlášení je neúspěšné. Identita nese ID uživatele (v tabulce *users* sloupec ID, který funguje jako primární klíč a automaticky se inkrementuje po přidání nového uživatele). Kvůli bezpečnosti se hesla neukládají do databáze ve formě plaintextu (v čitelné podobě), ale ukládá se pouze tzv. *hash* (otisk) hesla. Z tohoto *hashe* není možné získat původní heslo. K tomuto účelu slouží funkce *Passwords::hash($password)*, která nejdříve

heslo, které vyplní uživatel v přihlašovacím formuláři, zahešuje, a poté ho srovnává s hashem, kteý je uložený v databázi (při porovnávání se používá operátor ===, tedy neporovnává pouze hodnotu proměnné, ale i její datový typ). *Hash* hesla se generuje pomocí moderního algoritmu *bcrypt.*

Po úspěšném přihlášení je uživatel přesměrován na svůj vlastní dashboard, kde vidí všechny své aktivní úkoly v tabulce seřazené pod sebou. Při kliknutí na úkol se vedle tabulky zobrazí všechny informace o úkolu. Vlevo je menu obsahující všechny přístupné moduly (viz. níže). Vpravo nahoře je odkaz na uživatelův profil, kde si může editovat své vlastní uživatelské jméno a heslo.

Informační systém má tři základní moduly – projekty, uživatelé a úkoly.

Modul Uživatelé – v tomto modulu je přehledná tabulka všech uživatelů. Je zde možno vytvořit nové uživatele nebo editovat stávající. Uživatelé mají tři typy oprávnění (tabulka *users* má sloupec *role_id*, do kterého se ukládá cizí klíč na ID v tabulce r*oles*):

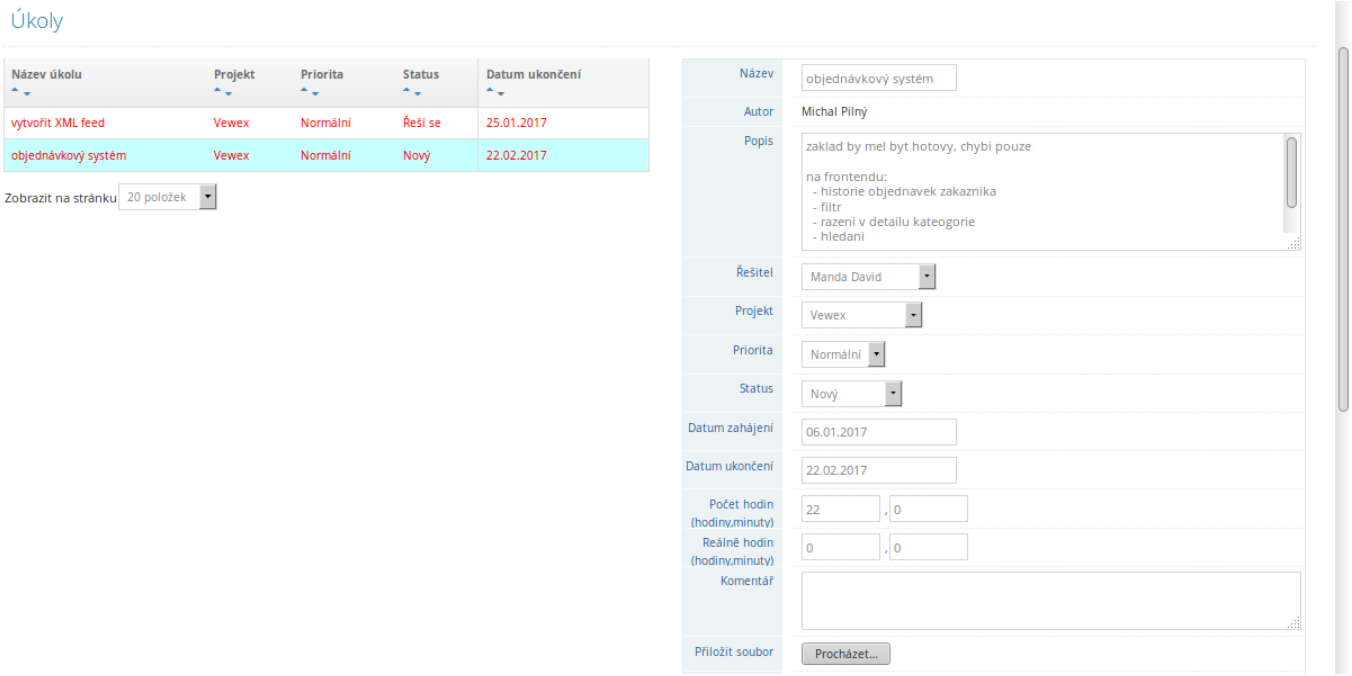
- administrátor – vidí a má přístup do všech modulů informačního systému
- zaměstnanec – vidí své úkoly i úkoly ostatních
- klient (vidí pouze úkoly z těch projektů, do kterých je přiřazen)

Do tohoto modulu mají přístup pouze administrátoři. Uživatele lze dočasně zneaktivnit (v uživatelském profilu může administrátor přepínat checkbox aktivní/neaktivní). Takoví uživatelé se poté nebudou moci do informačního systému přihlásit. Uživatelé lze taky smazat (smaže se jeho záznam v tabulce *users*).

Modul Projekty – tento modul obsahuje tabulku všech projektů. Do tohoto modulu mají přístup pouze administrátoři. Je zde možné vytvářet nové projekty nebo editovat již existující. Každému projektu je možno nastavit hlavního řešitele z nabízených zaměstnanců, a taky více emailových adres (funkčnost bude vysvětlena níže).

Modul Úkoly – do tohoto modulu mají přístup všechny role, klienti zde ovšem mají hodně omezenou pravomoc. Po kliknutí na modul v nabídce vlevo nejdříve vyjede seznam všech zaměstnanců, po vybrání zaměstnance se poté zobrazí dashboard se všemi úkoly, které

zaměstnanec momentálně řeší. Pokud se uživatel přihlásí, je přesměrován rovnou na svůj dashboard (viz. obr 6).



Obr. 6 Modul Úkoly

Každý úkol má několik údajů – název, autor úkolu, popis, řešitel, projekt, priorita, status, datum založení, datum ukončení, počet hodin a počet reálných hodin. Pod každým úkolem je taktéž možno vkládat soubory a přidávat komentáře. Zde jsou uvedeny možnosti údajů, které lze u úkolů nastavovat:

- priorita – nízká, normální, vysoká
- status – nový, řeší se, ke schválení, vyřešeno, čeká se

Výchozí řazení úkolů v dashboardu závisí na datu ukončení a na prioritě (úkoly s nejstarším datem ukončení a nejvyšší prioritou budou nejvýše). Každý uživatel si může své úkoly seřadit podle:

- názvu úkolu
- projektu

- priority
- statusu
- datu ukončení.

Díky knihovně MailLibrary [12] je dokonce umožněno, aby klienti nemuseli vůbec vstupovat do informačního systému. Tato knihovna je díky třídě ImapDriver schopna se připojit k firemnímu emailu, a odtud do informačního systému stáhnout všechny emaily. Stačí tedy, aby klient napsal na info@nazev_firmy.cz, a i v informačním systému se založí nový úkol (název emailu se převede na název úkolu a tělo emailu se vloží do popisu úkolu). Pokud bude emailová adresa u projektu uložena, tak se úkol vloží přímo hlavnímu řešiteli projektu. Úkoly z neznámých emailů se vloží do záložky *Nepřiřazené úkoly*. Knihovna MailLibrary se spouští v tzv. *cronu*, což je v podstatě funkce, která automatizovaně v určitý čas spouští nějaký příkaz.

5.4 SWOT ANALÝZA INFORMAČNÍHO SYSTÉMU

SWOT analýza informačního systému slouží k identifikaci silných, slabých stránek, příležitostí a hrozeb.

Silné stránky

- přehlednost systému
- systém dostupný odkudkoliv přes internet
- do systému mohou i klienti firmy
- klienti mohou zakládat úkoly i přes email
- v systému mohou být neomezený počet uživatelů, projektů i úkolů

Slabé stránky

- informační systém nepoužívají všichni klienti firmy
- majitel firmy dostatečně nebere v potaz zpětnou vazbu zaměstnanců na IS
- neběží na *https* protokolu
- interní školení zaměstnanců

Příležitosti

- zavedení nových bezpečnostních pravidel
- zavedení pravidel pro práci s IS pro zaměstnance i pro klienty
- vytvoření nového modulu přívětivého pro klienty

Hrozby

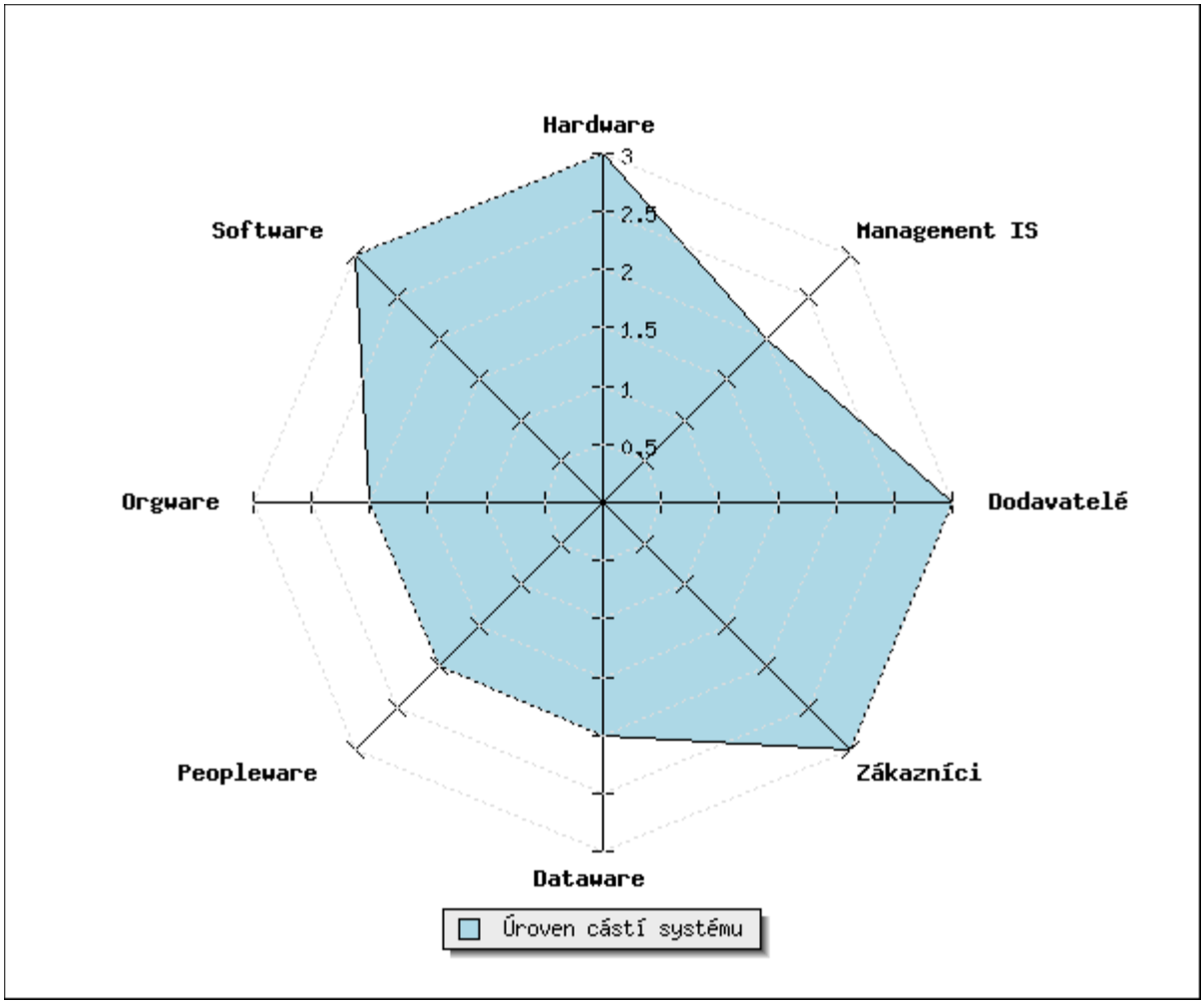
- ztráta citlivých dat
- útoky přes emaily zakládající úkoly

5.5 ANALÝZA METODOU HOS 8

Tato kapitola se zabývá analýzou stávajícího informačního systému metodou HOS 8. Tato analýza byla provedena za pomoci informačního systému Zefis [13]. Portál Zefis slouží k posouzení informačních systémů a vyhledávání jeho slabých míst. Analýza zkoumaného systému byla provedena pomocí jednoho dotazníku, který vyplňoval zaměstnanec společně s autorem práce.

5.5.1 Úroveň částí systému

Z následujícího grafu (viz. graf 1) je zřejmé hodnocení jednotlivých částí systému. Jedná se o pavučinový graf s osmi osami, které znázorňují jednotlivé zkoumané části informačního systému. Úroveň každé z oblastí je ohodnocena pomocí čtyřbodové škály jako **1- špatná, 2 -spíše špatná, 3 - spíše dobrá 4 - dobrá**.



Graf 1 Úroveň částí systému (exportováno z portálu Zefis [13])

5.5.2 Hardware

Tato oblast je ohodnocena úrovní 3 – spíše dobré. Je to především proto, že veškeré hardwarové vybavení bylo pořízeno poměrně před nedávnou dobou, a celkově prošlo velkou obměnou. Rozhodně není žádné hardwarové zařízení starší více než dva roky.

Všichni zaměstnanci společnosti dostávají firemní notebook značky *Asus Zendbook*. S těmito notebooky je značná spokojenost. Nejvíce notebooků ve firmě má tyto parametry:

- Úhlopříčka displeje ["]: **13,3**
- Typ procesoru: **Intel Core i3**

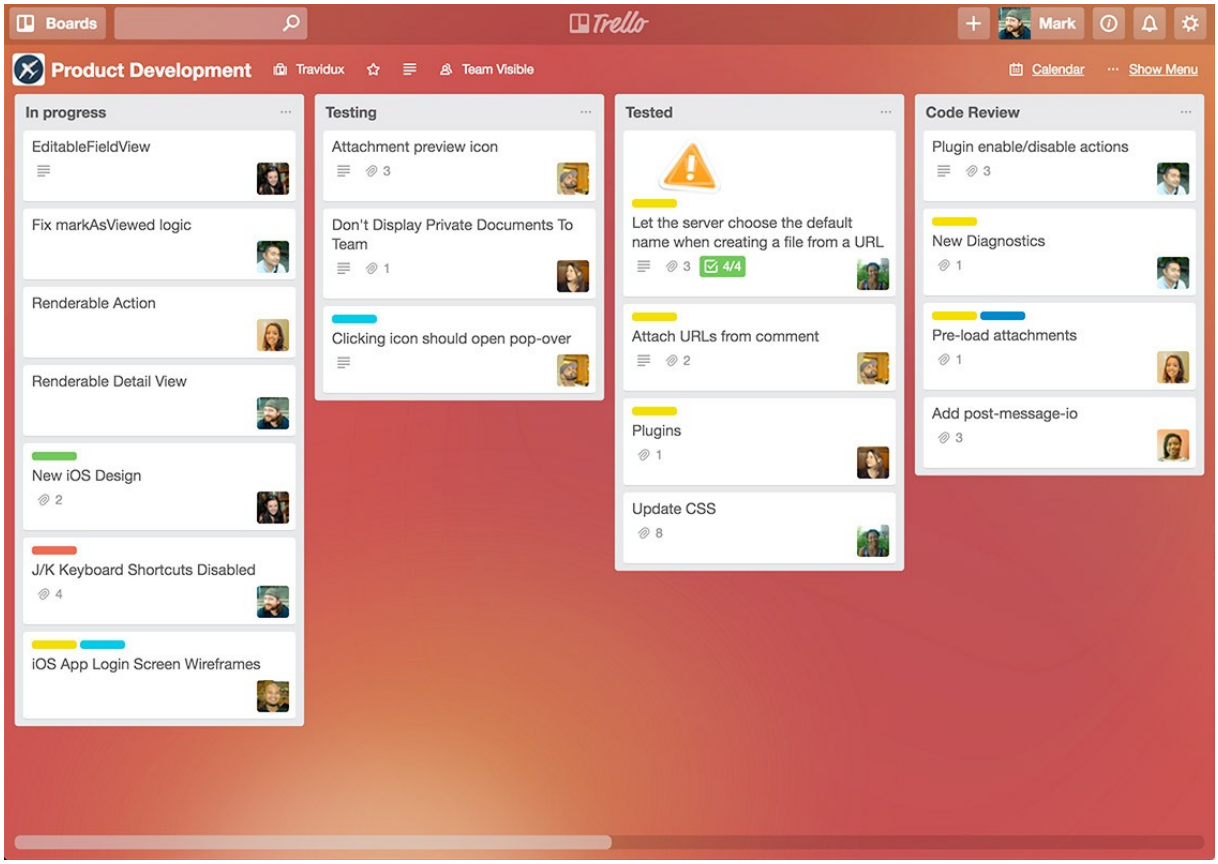
- Model procesoru: **6100U(2.3GHz 2jádra/4vlákna)**
- Počet jader procesoru: **2**
- Interní paměť [GB]: **500**
- Grafická karta: **Intel HD Graphics**
- Velikost operační paměti [GB]: **4**
- Rozlišení displeje: **1366 x 768 (HD)**

Co se týká serverového vybavení, tak i při vyšší zátěži zvládají vyřizovat požadavky v požadovaném čase. Připojení k internetu je taktéž na slušné úrovni, výpadky jsou jen velmi vzácné.

5.5.3 Software

Samotný používaný software je také hodnocen stupněm 3 – spíše dobrý. Tato oblast ve společnosti poskytuje všechny potřebné funkce, které jsou nezbytné pro práci zaměstnanců. Informační systém je přehledný a uživatelům usnadňuje práci.

Jednu slabou stránku přesto SWOT analýza informačního systému zachytila. Jeden z největších a nejdůležitějších klientů firmy odmítá používat informační systém, protože dává přednost systému *Trello*, což je webová aplikace pro řízení projektů, kde jsou úkoly zastoupeny „nástěnkami“ rozdělenými do sloupců. Úkoly lze v rámci sloupců posouvat pomocí *drag-and-drop*, což informační systém neumožňuje. Pro zaměstnanci je nepříjemné, že musí v podstatě sledovat dva systémy, protože ostatní klienti zakládají úkoly do informačního systému. Proto bude v tomto případě navržena změna v kapitole 6.



Obr. 7 Ukázka Trella [14]

Další programy, které se ve firmě používají – PHPStorm, Gimp, Mozzila Thunderbird, Jabber atd.

5.5.4 Orgware

Tato oblast je na tom podle analýzy HOS 8 již hůře. Je ohodnocena stupněm 2 – spíše špatná. Společnost nemá existující postupy či směrnice pro řešení nestandardních a havarijních situací informačních systémů. Stejně tak neexistují bezpečnostní pravidla informačního systému. Firma také nepořádá pro zaměstnance pravidelná školení na práci se systémem.

5.5.5 Peopleware

Tato oblast je ohodnocena stupněm 2 – spíše špatná. Ve firmě nejsou dostupná školení pracovníků o používaném informačním systému. Systém však není příliš komplikovaný a zaměstnanci si s ním zatím vždy poradili.

Neexistuje zastupitelnost koncových uživatelů, kteří jsou klíčoví pro chod systému.

V posledních měsících jsou zaměstnanci přetížení, dodržování termínů už začíná být „na hraně“.

5.5.6 Dataware

Ve společnosti neprobíhá pravidelné zálohování dat uložených na lokálních počítačích pracovníků. Zálohování dat na serveru má na starosti firma Wedos, takže pravděpodobnost ztráty nebo zcizení dat je celkem malá. Ve firmě neexistují podrobné plány pro obnovu klíčových dat v informačním systému v případě jejich poškození nebo zničení. I z těchto důvodů je tato oblast ohodnocena stupněm 2 – spíše špatná.

5.5.7 Zákazníci

Společnost má stálé a platově spolehlivé zákazníky. Neexistují metriky cílů informačního systému směrem k zákazníkům. Klienti mají přístup do informačního systému a mohou zde zakládat úkoly zaměstnancům. Tato oblast má v analýze HOS 8 hodnocení stupeň 3 – spíše dobrý.

5.5.8 Dodavatelé

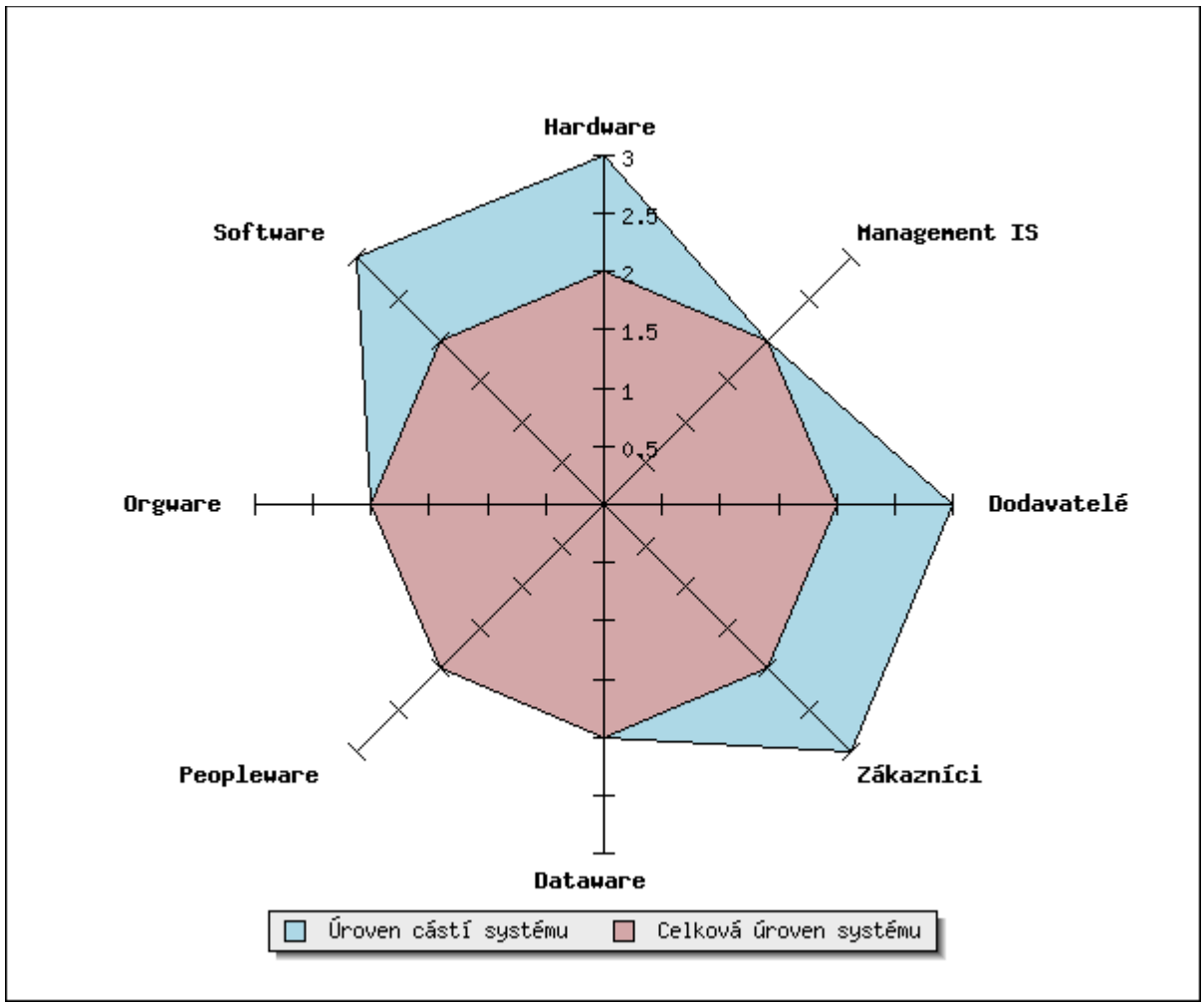
Tato oblast je ohodnocena úrovní 3 – spíše dobré. Dodavatelem informačního systému jsou zákazníci firmy, protože systém je vlastní interní projekt. Z tohoto důvodu není potřeba s dodavatelem webového systému podepisovat *SLA* ani *OLA*.

5.5.9 Management IS

Majitel společnosti si uvědomuje důležitost informačního systému pro chod firmy, v podstatě systém vznikl díky jeho iniciativě, a celý návrh systému vytvořil on sám. Horší je to s odezvou zaměstnanců na spokojenost se systémem, se kterými se do teď moc nezabýval. Zaměstnanci firmy by si přáli pár menších úprav. Firma nemá v této oblasti definovanou informační strategii, ani pravidla pro práci a bezpečnost. Tato oblast je ohodnocena úrovní 3 – spíše dobré.

5.5.10 Celkový stav systému

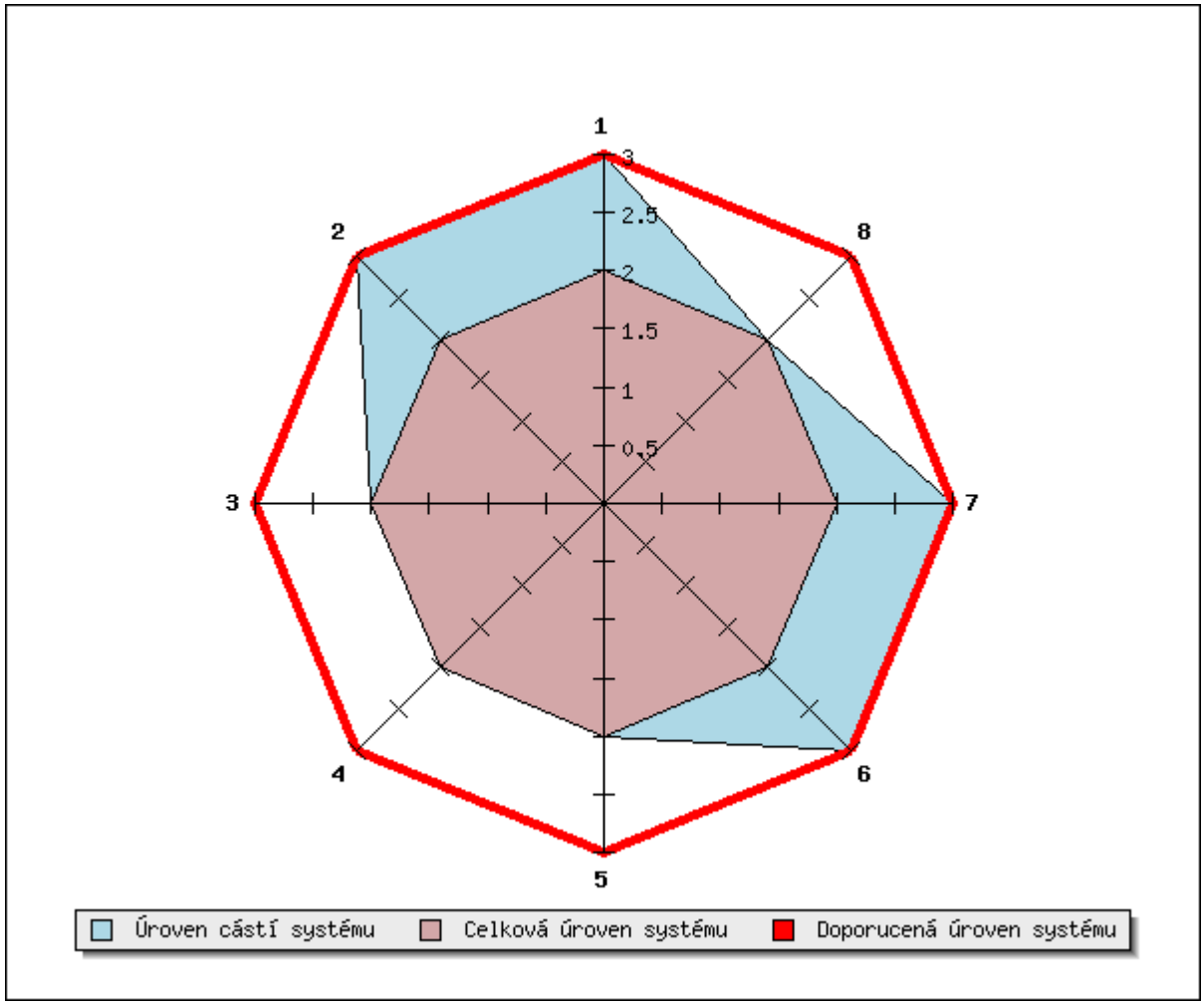
Celková úroveň systému je dána jeho nejslabším článkem. Podle analýzy HOS 8 je celková úroveň informačního systému 2 - spíše špatná úroveň. Celková úroveň informačního systému je znázorněna v grafu růžovou oblastí.



Graf 2 Celkový stav systému (exportováno z portálu Zefis [13])

5.5.11 Doporučený stav systému

Z provedené analýzy HOS 8 vyplývá, že doporučená úroveň všech částí informačního systému by měla být na stupni 3 - dobrý. Tato hodnota je odvozena od důležitosti systému. Doporučená úroveň informačního systému je znázorněna červeným osmiúhlelníkem v grafu. Celková úroveň informačního systému je znázorněna růžovou oblastí v grafu.

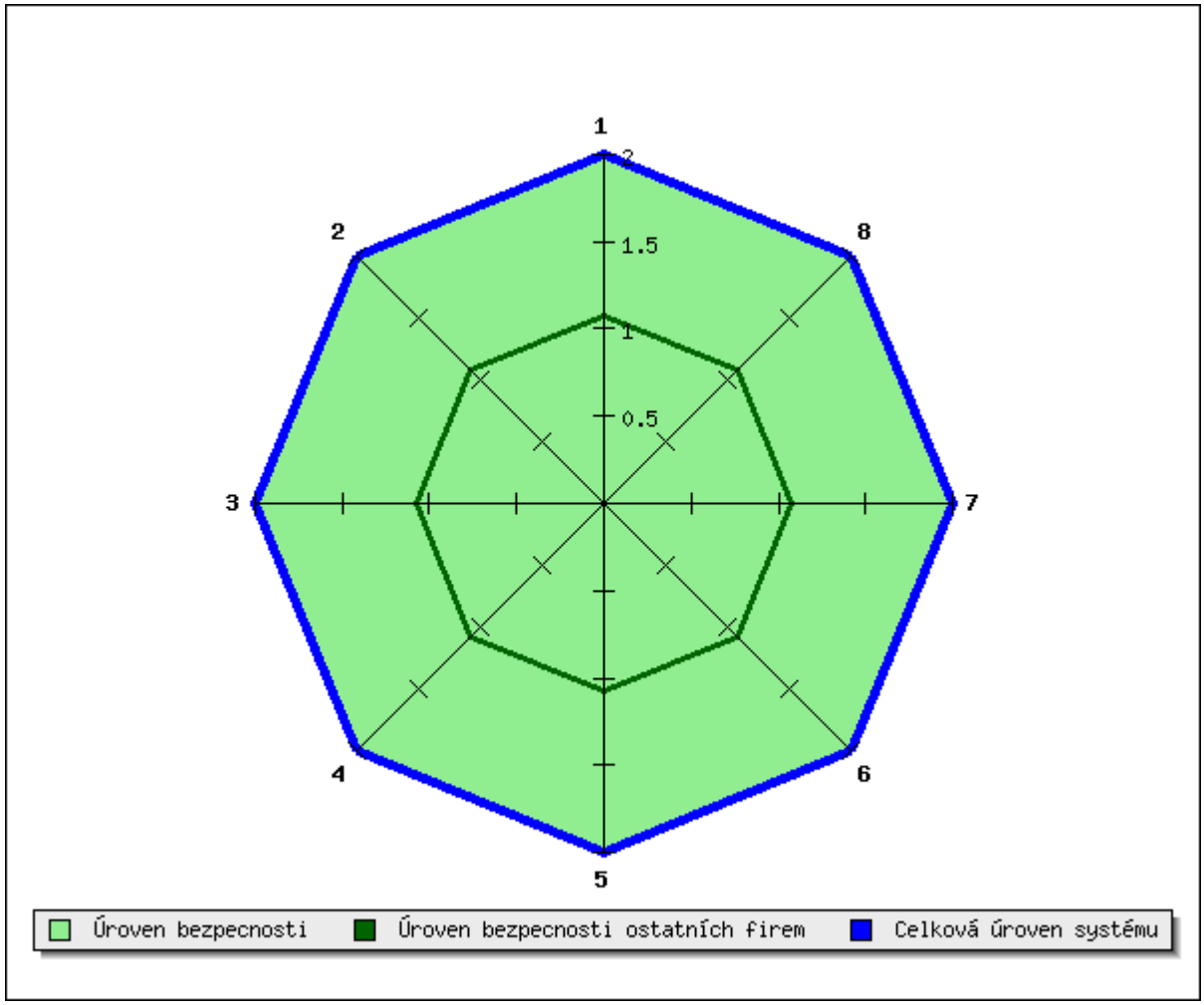


Graf 3 Doporučený stav systému (exportováno z portálu Zefis [13])

5.5.12 Informační bezpečnost

Analýza HOS 8 ohodnotila informační bezpečnost společnosti hodnotou 2, tedy jako spíše špatnou úroveň. Úroveň informační bezpečnosti je znázorněna zelenou oblastí v grafu. Celková úroveň informačního systému je znázorněna tlustou modrou čarou v grafu.

Ve společnosti není zavedená norma ISO 27000 (Systém řízení bezpečnosti informací). Někteří zaměstnanci si nezamykají pracovní plochu, když odcházejí mimo kancelář.



Graf 4 Informační bezpečnost (exportováno z portálu Zefis [13])

6 VLASTNÍ NÁVRHY ŘEŠENÍ

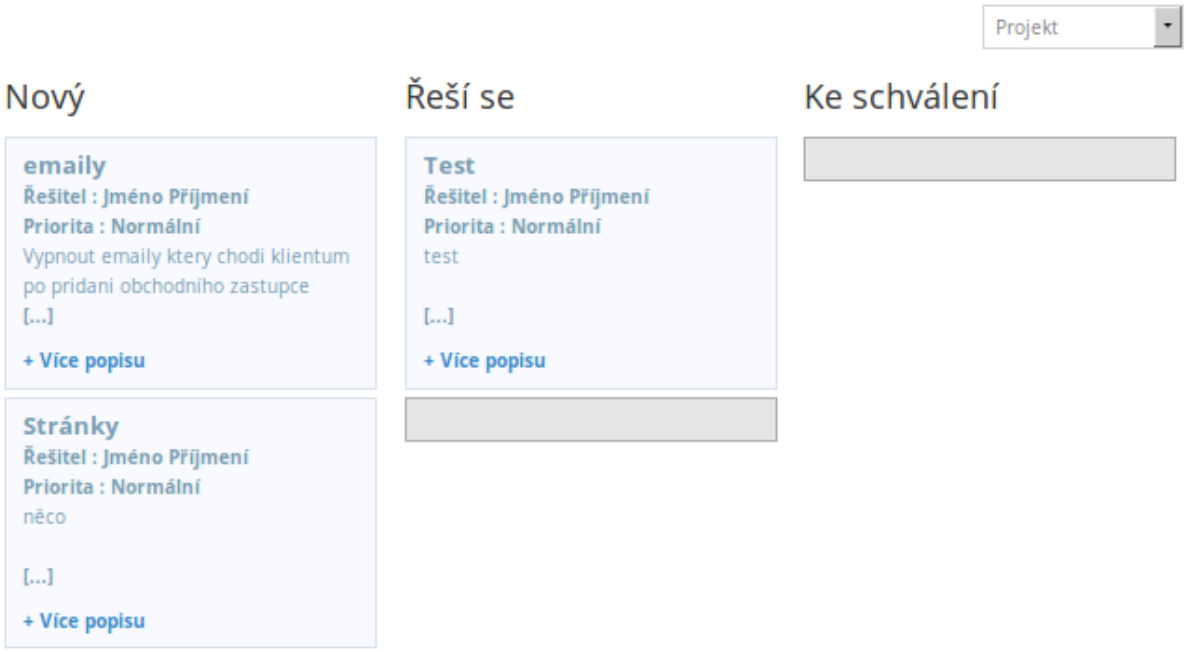
Tato kapitola shrnuje návrhy vlastních řešení, které by se mohly provést, a které by mohly zajistit zvýšení efektivnosti a celkové hodnocení informačního systému metodou HOS 8.

6.1 ZMĚNY V OBLASTI SOFTWARE

6.1.1 Nový modul Úkoly - přehled

Jak už bylo řečeno výše, jeden z hlavních klientů místo informačního systému raději používá webovou aplikaci *Trello*, protože mu vyhovuje drag-and-drop přesouvání úkolů. Po domluvě s klientem je navržen nový modul, který by mu vyhovoval, a samozřejmě by ho mohli požívat i ostatní klienti, a zaměstnanci společnosti by tento modul taktéž rádi používali.

Funkčnost by měla být následující – po kliku na modul by se měla objevit nová stránka, kde bude *select* se všemi projekty. Po vybrání projektu se načtou všechny úkoly z projektu, a rozdělí se do sloupců podle statusů úkolů. Statusy u úkolů jsou: nový, řeší se, ke schválení, vyřešeno, čeká se. Celkem tedy bude pět sloupců, mezi kterými bude možnost úkoly pomocí myši přesouvat. Návrh modulu je na obr. 8



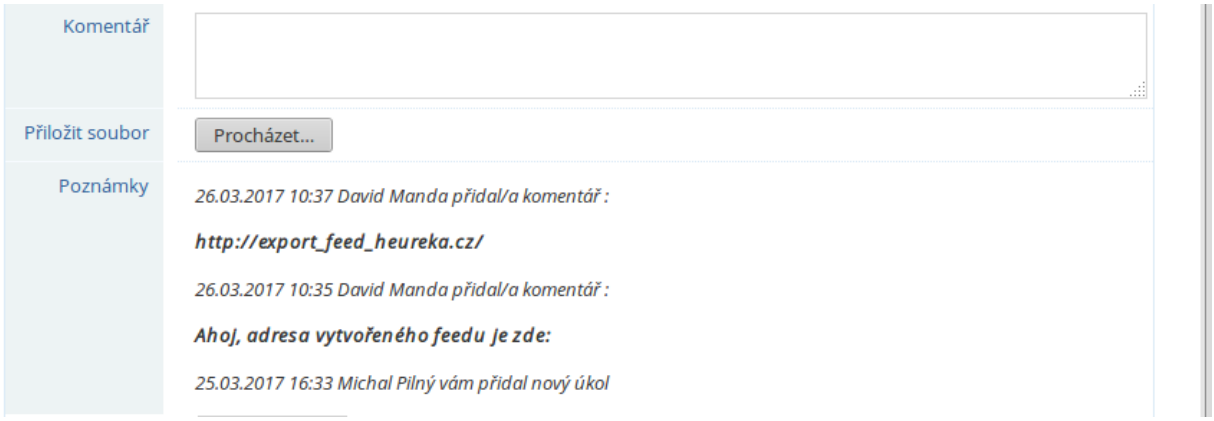
Obr. 8 Návrh modulu Úkoly - přehled

Dle mého názoru by funkčnost drag-and-dropu bylo možné udělat pomocí javascriptové knihovny j*Query*, která se již v projektu používá (nebylo by třeba načítat jiné knihovny), *a* která obsahuje funkci *sortable* [15]. Pokud by byl celý sloupec obalený do *divu*, a tomuto *divu* by byla přidělena nějaká třída, např. * *, potom by se v javascriptovém kódu dala na této třídě zavolat požadovaná funkce *sortable*, např. *$(".dd-list").sortable({})*

Úprava v dosavadní databázi by nebyla třeba, po přesunu úkolu do jiného sloupce se změní status úkolu, který už v databázi existuje. Celkovou náročnost implementace modulu včetně testování odhaduji na 4 pracovní dny, tedy na 32 hodin.

6.1.2 Úprava přidávání komentářů

Z rozhovorů se zaměstnanci vyplynulo, že několik je jich nespokojených s přidáváním komentářů pod úkoly. Pro komentáře je zde umístěna *textarea*, do které zaměstnanec napíše text, který se potom odešle při kliknutí kamkoliv myší. Tuhle funkcionalitu zajišťuje funkce *change()* z knihovny Jquery. Je možné ji použít i na jiné *HTLM* elementy, např. na *select* nebo *input.* V tomto případě se komentář odešle ihned, jakmile se změní hodnota elementu *textarea* a klikne se myší mimo tento element. Je to chtěná funkce navržená pro rychlé odesílání komentářů (nemusí se klikat na žádné tlačítko pro odeslání). To ale na druhou stranu může způsobovat potíže v momentě, kdy chce uživatel např. do rozepsaného komentáře z nějakého jiného místa zkopírovat jiný text. Ukázka, kdy se komentář rozdělí na zbytečné dvě části, je na obrázku 9. Výsledkem může být zmatek v komentářích.



Obr. 9 Ukázka přidávání komentářů

Pro tento problém navrhuji následující řešení: do profilu uživatele bych přidal nový *checkbox*, jehož *label* by měl „Zobrazit tlačítko na komentáře“. Každý uživatel tedy bude mít na výběr, jestli chce nebo nechce odesílací tlačítko na komentáře. Do tabulky *users* by pouze přibyl jeden sloupec, do kterého by se ukládalo, zda je nebo není checkbox zaškrtnutý. S navrženou změnou majitel firmy souhlasí. SQL dotaz by mohl vypadat následovně:

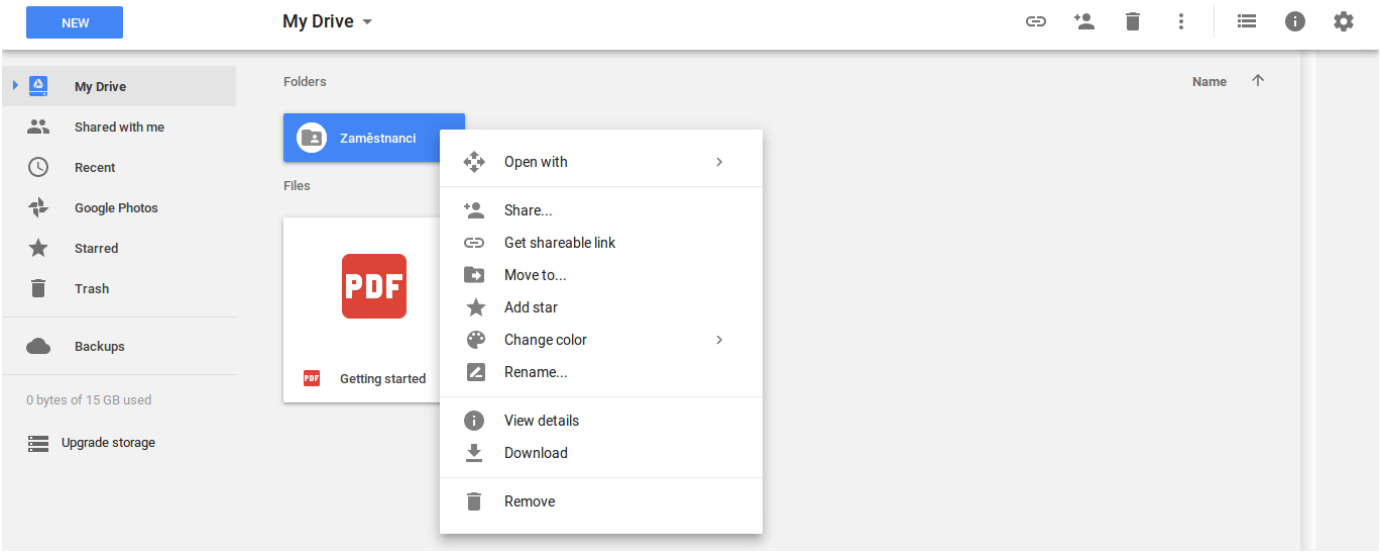
```
ALTER TABLE `users` ADD `send_button` TINYINT NOT NULL DEFAULT '0' AFTER `email`;
```

V modulu Úkoly by potom byla podmínka, zda se má odesílací tlačítko zobrazit nebo nezobrazit podle hodnoty uložené v databázi. Stejně tak se musí opodmínkovat kód v Javascriptu na funkci *change()*. Výchozí nastavení bude tlačítko nezobrazovat. Náročnost této úpravy bych odhadoval na 7 hodin.

6.2 ZMĚNY V OBLASTI DATAWARE

Ve společnosti neprobíhá pravidelné zálohování dat uložených na lokálních počítačích pracovníků. Z tohoto důvodu navrhuji do společnosti zavedení služby *Google Drive*, která poskytuje cloudové řešení jak pro firmy, tak i pro osobní účely. Navrhuji založit jeden firemní účet, na kterém se budou sdílet soubory a složky, do kterých budou zaměstnanci zálohovat své data. Každý zaměstnanec uvidí pouze ty složky, které mu budou ve firemním účtu zpřístupněny (o sdílení složek a souborů bude nejspíše rozhodovat majitel firmy).

Tato služba umožňuje ukládat všechny různé soubory - články, návrhy, nákresy, zvukové nahrávky i videa. Pro účely společnosti by bohatě postačoval disk s velikostí 1 TB za 299,99 CZK za měsíc. Ukázka služby je na obrázku 10.



Obr. 10 Ukázka *Google Drive [16]*

6.3 ZMĚNY V OBLASTI BEZPEČNOSTI

Tuto oblast analýza HOS 8 ohodnotila hodnotou 2, tedy jako spíše špatnou úroveň. Následující kroky by měly oblast informační bezpečnosti zvýšit.

6.3.1 Šifrování a podepisování emailů

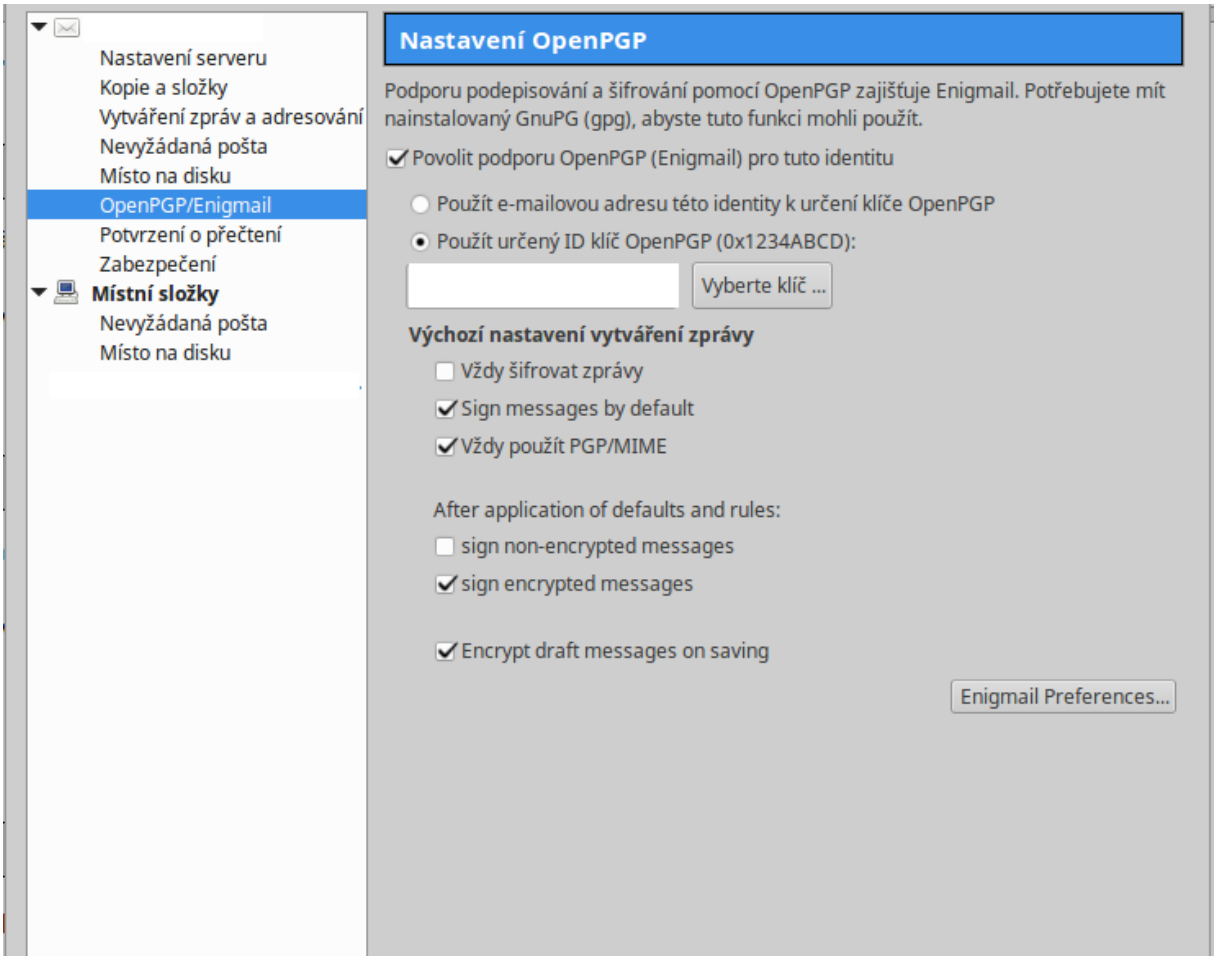
Pro šifrování a podepisování emailů bych zvolil program *GPG* (*GNU Privacy Guard)*, který umí šifrovat a dešifrovat data, elektronicky podepisovat a podpis zpětně ověřovat. Tento program je nástupcem *PGP (Pretty Good Privacy).* Klíč se vygeneruje příkazem

gpg2 –gen-key

Po vygenerování nového klíče získáme mimo jiné i ID klíče, pomocí kterého klíč nahrajeme na keyserver, což je shromaždiště veřejných klíčů.

gpg2 –send-keys <ID_HLAVNIHO_KLICE>

Z keyserveru poté importujeme klíče spolupracovníků. Všichni zaměstnanci společnosti používají emailového klienta *Mozilla Thunderbird*. Pomocí rozšíření *Enigmail* můžeme používat *GPG* program přímo v tomto emailovém klientovi (viz. obr. 11).



Obr. 11 *Mozilla Thunderbird*

6.3.2 Přechod na HTTPS protokol

V současné době beží informační systém pod *HTTP* certifikátem, což není úplně ideální. *HTTP* (*HyperText Transfer Protokol*) zajišťuje komunikaci mezi webovým prohlížečem a vzdáleným serverem. Tato komunikace však není šifrovaná a přenášené informace může po cestě mezi prohlížečem a serverem kdokoliv číst, včetně hesel a dalších citlivých údajů, které uživatelé vyplňují ve formulářích. Právě z tohoto důvodu byl vyvinut

HTTPS (anglicky *Secured*, zabezpečený) protokol, který zajišťuje šifrovanou komunikaci.

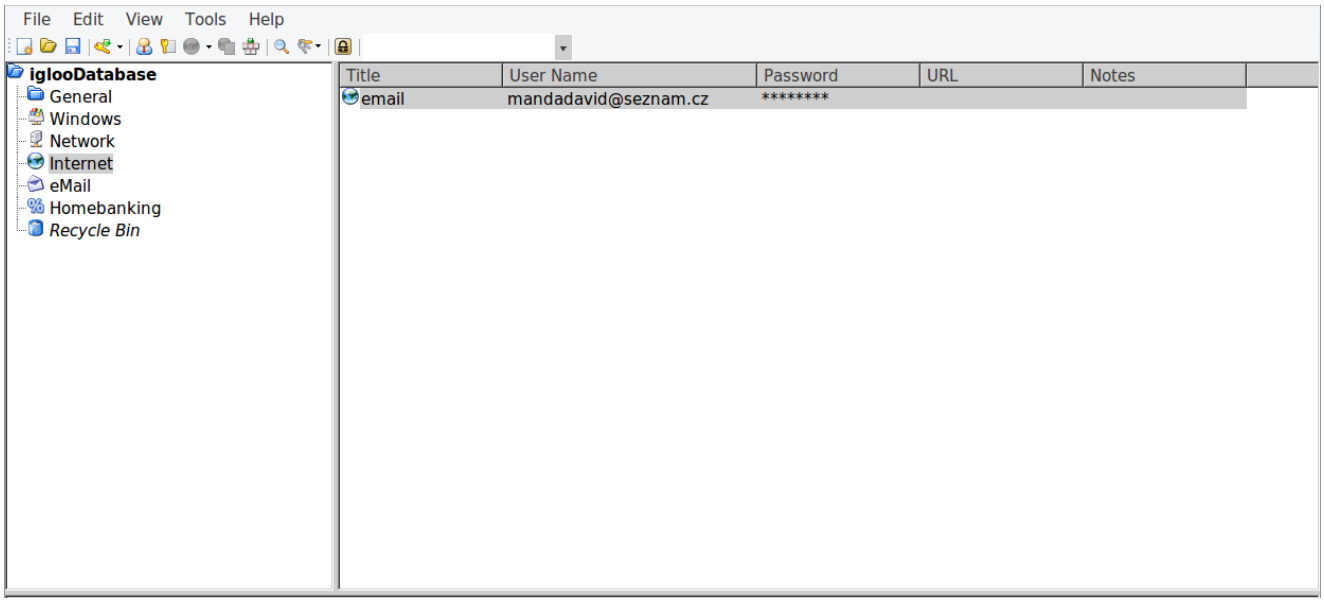
Pro zavedení *HTTPS* protokolu je nutné nainstalovat *SSL* certifikát. Některé hostingy poskytují *HTTPS* certifikát zcela zdarma. Dále je nutné uzpůsobit informační systém. V Nette Frameworku to není nic složitého. Musí se pouze upravit soubor *RouterFactory.php,* tedy přizpůsobit routy na *HTTPS* protokol. Dobu na provedení této úpravy bych odhadoval na 2 hodiny.

6.3.3 Escapování emailů od klientů

Při průzkumu kódu informačního systému byla nalezena možná zranitelnost. Systém pomocí knihovny *MailLibrary* stahuje emaily od klientů a na jejich základě zakládá nové úkoly. Tyto vstupy od klientů ale nejsou žádným způsobem *escapovány,* což může být využito útočníky (např. pro útok *XSS*). *Escapování* je převod znaků majících v daném kontextu speciální význam na jiné odpovídající sekvence. V *PHP* je speciální funkce na *escapování* znaků, a to *htmlspecialchars*(*string $string*). Doporučuji tedy tuto funkci doplnit na potřebná místa. Dobu na provedení této úpravy bych odhadoval na 1 hodinu.

6.3.4 Používaní klíčenky

Pro správu hesel doporučuji používání klíčenky. Klíčenku mohou požívat všichni zaměstnanci a hlavní výhoda spočívá v tom, že si zaměstnanec nebude muset pamatovat žádné hesla (samozřejmě kromě hesla do klíčenky). Kvalitní klíčenkou je např. *KeePass,* což je program, který je určen k uschování všech hesel a přihlašovacích údajů, které uživatel používá a to vše pod jedním hlavním kódem. Hesla lze uspořádat do přehledných skupin (viz. obr. 12)



Obr. 12 *KeePass*

6.4 ZMĚNY V OBLASTI ORGWARE

Situace společnosti je momentálně taková, že ve firmě neexistují bezpečnostní pravidla informačního systému, a také se nepořádají pro zaměstnance žádná pravidelná školení na práci se systémem.

Z tohoto důvodu navrhuji vypracování nové bezpečnostní politiky, kterou vytvoří majitel společnosti. Výstupem by měl být dokument, kterým by se měli zaměstnanci řídit. Navrhuji následující témata a pravidla, kterých by se měla bezpečnostní politika společnosti držet:

- šifrování a podepisování emailů
- používání spolehlivých antivirových programů
- používání silných hesel
- používání klíčenky
- uzamykání notebooků vždy, když od něj zaměstnanec odejde
- šifrování disků

Hesla by se neměla ukládat v otevřené podobě, měla by být v zašifrované podobě v

klíčence. Pokud se heslo posílá emailem, je nutno email zašifrovat systémem *GPG*.

6.5 ZMĚNY V OBLASTI PEOPLEWARE

V posledních měsících jsou zaměstnanci přetížení, dodržování termínů už začíná být „na hraně“. Doporučoval bych tedy přijmout nového vývojáře (programátora). Mohlo by jít klidně i o šikovného absolventa nebo studenta, který by nastoupil na poloviční úvazek.

6.6 ZMĚNY V OBLASTI MANAGEMENTU

Z důvodu časového vytížení se v současné době nekonají žádné porady mezi zaměstnanci a vedením společnosti. Tím mohou nastat zbytečné konflikty a nedorozumění, který by se přitom daly lehce vyřešit na poradách. Proto navrhuji konat pravidelné porady v určitý den a hodinu každé dva až tři týdny.

6.7 EKONOMICKÉ ZHODNOCENÍ

Nejnákladnější položkou je vyhotovení modulu Úkoly – přehled. Ekonomické zhodnocení počítá s hodinovou sazbou pro programátora 250 Kč. Přehled nákladů jsou zobrazeny v tabulce 1.

Položka	**Počet hodin**	**Náklady (v Kč)**
Modul Úkoly - přehled	32	8000
Úpravy přidáváni komentářů	7	1750
Google Drive	-	299,99
Zavedení HTTPS	2	500
Escapování vstupů	1	250
Celkem	-	10500 Kč + 299,99 Kč/měs

Tab. 1 Tabulka ekonomického zhodnocení

Celkové náklady na uskutečnění návrhů představují částku 10 500 Kč, plus ještě náklad 299,99 Kč za měsíc za cloudovou službu. Podle mého názoru změny zmíněné v kapitole 6 budou pro společnost přínosem a také budou mít vliv na eliminaci rizik.

7 ZÁVĚR

Tato diplomová práce Posouzení informačního systému u vybrané firmy a návrh změn se snaží přispět ke stále aktuálnější problematice informačních systémů ve firmách a organizacích. Hlavním cílem bylo analyzovat zavedený informační systém internetové agentury a najít jeho hrozby, a poté navrhnout vhodné změny ke zlepšení systému společnosti.

Třetí kapitola této práce popisuje úvod do teorie systémů, vysvětluje pojmy systémový přístup a systémové myšlení.

Čtvrtá kapitola popisuje informační systémy, rozebírá pojmy data, informace a znalosti. Podkapitola Bezpečnost informačních systémů je zaměřena na hrozby a útoky v informačních systémech, jsou zde vysvětleny pojmy virus, červ, trojský kůň a rootkit. Konec kapitoly se zabývá technologiemi při implementaci informačních systémů.

Pátá kapitola práce má za úlohu představení společnosti, analyzovat současný stav situace a přestavit informační systém, který se ve firmě používá. V rámci kapitoly je taktéž vyhodnocení metodou HOS 8.

Poslední šestá kapitola shrnuje návrhy vlastních řešení, které by se mohly provést, a které by mohly zajistit zvýšení efektivnosti a celkové hodnocení informačního systému

8 SEZNAM POUŽITÉ LITERATURY

[1] BASL, J., BLAŽÍČEK, R. Podnikové informační systémy: Podnik v informační společnosti. 3. aktual. vydání Praha: Grada Publishing, 2012. 323 s. ISBN 978-80-247-4307-3.

[2] MOLNÁR, Zdeněk. Efektivnost informačních systémů. 1. vydání. Praha : Grada Publishing, 2000. 144 s. ISBN 80-7169-410-X.

[3] JANÍČEK, Přemysl. Systémová metodologie: brána do řešení problémů. Vyd. 1. Brno: Akademické nakladatelství CERM, 2014, [365] s. v různém stránkování. ISBN 978-80-7204-887-8.

[4] KOCH, M., DYDOWICZ, P., ONDRÁK, V., KŘÍŽ, J., HAJKR, J. Informační systémy a technologie. 2. vyd. Brno: Akademické nakladatelství CERM, 2002. 151 s. ISBN 80-80-214-2193-2.

[5] DOSKOČIL, R., KORÁB, V. Znalostní management. 1. vyd. Brno: Akademické nakladatelství CERM, 2012. 130 s. ISBN 978-80-214-4668-7.

[6] RÁBOVÁ, Ivana. *Podnikové informační systémy a technologie jejich vývoje*. V Tribun EU vyd. 1. Brno: Tribun EU, 2008. 139 s. ISBN 978-80-7399-599-7

[7] HANÁČEK, P. STAUDEK, J.: *Bezpečnost informačních systémů.* Úřad pro státní informační systém, 2000. 127p.

[8] SKOUDIS, E.: *Malware – Fighting Malicious Code.* New Jersey, 2004. 650p. ISBN 0-13-101405-6.

[9] RAIS, K., DOSKOČIL, R. Risk management. 1. vyd. Brno: Akademické nakladatelství CERM, 2007. 152 s. ISBN 978-80-214-3510-0.

[10] KOSEK, J. PHP – tvorba interaktivních internetových aplikací. 1. vydání. Praha : Grada Publishing, 1998. 492 s. ISBN 80-7169-373-1

[11] Nette Framework [Online] [cit. 2017-04-26] Dostupné z: https://doc.nette.org/cs/2.4/quickstart/getting-started.

[12] MailLibrary [Online] [cit. 2017-05-01] Dostupné z: https://github.com/greeny/MailLibrary

[13] KOCH, Miloš. Posouzení vyváženosti IS metodou HOS 8. ZEFIS [online]. 2014 [cit. 2017-05-10]. Dostupné z: http://www.zefis.cz/zefis/zefis.php

[14] Trello [online]. [cit. 2017-05-13]. Dostupné z: https://trello.com/

[15] Jquery [online]. [cit. 2017-05-13]. Dostupné z: https://jqueryui.com/sortable/

[16] Google Drive [online]. [cit. 2017-05-16]. Dostupné z: https://www.google.com/drive/

9 SEZNAM OBRÁZKŮ

10 SEZNAM TABULEK A GRAFŮ

11 SEZNAM ZKRATEK A SYMBOLŮ

EIS - Executive Information Systems

MIS - Management Information Systems

DSS - Decision Support Systems

TPS - Transaction Processing Systems

CRM - Customer Relationship Management

ERP - Enterprise Resource Planning

GIS - Geographic Information System

CAM - Computer Aided Manufacture

EDI - Electronic Data Interchange

OIS - Office Information System

PHP - Hypertext Preprocessor

HTML - HyperText Markup Language

GPG - GNU Privacy Guard

PGP - Pretty Good Privacy

HTTP - HyperText Transfer Protokol