Vysoká škola ekonomická v Praze

Fakulta managementu v Jindřichově Hradci

Bakalářská práce

Petr Novák

2007

Vysoká škola ekonomická v Praze

Fakulta managementu Jindřichův Hradec

Bakalářská práce

Petr Novák

2007

VŠE

FAKULTA MANAGEMENTU

Vysoká škola ekonomická v Praze
Jarošovská 1117/II, 377 01 Jindřichův Hradec

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

pro akademický rok 2006/2007

Název práce:	**IS/IT Edscha Tools a.s.**
Zadání práce:	Práce se bude zabývat IS/IT Edscha Tools, a.s. a to z hlediska bezpečnosti a ochrany dat, využití IS organizace při plánování výroby a komunikace se zákazníkem, možnostmi rozšíření IS/IT pro zaměstnance a vedení firmy.
Jméno studenta:	Petr Novák
Ročník:	2.
Obor:	MANAGEMENT
Vedoucí práce:	Ing. Pavel Pokorný
Katedra:	Katedra managementu informací
Termín zadání:	23.6.2006
Termín odevzdání:	Dle vyhlášky o průběhu státních závěrečných zkoušek v ak. roce 2006/2007

V Jindřichově Hradci 23.6.2006

Ing. Vladimír Přibyl
proděkan pro pedagogickou činnost

tel.: 384 417 200 fax: 384 417 277 IČ: CZ61384399 bank. spoj. ČSOB a. s. J. Hradec č. ú. 170922147/0300

Vysoká škola ekonomická v Praze

Fakulta managementu v Jindřichově Hradci

IS/IT Edscha Tools a.s.

Vypracoval:

Petr Novák

Vedoucí bakalářské práce:

Ing. Pavel Pokorný

J. Hradec, červen 2007

Prohlášení

Prohlašuji, že bakalářskou práci na téma

IS/IT Edscha Tools a.s.

jsem vypracoval samostatně.

Použitou literaturu a podkladové materiály

uvádím v přiloženém seznamu literatury.

J. Hradec, červen 2007

.....

podpis studenta

Anotace

IS/IT Edscha Tools a.s.

Práce se zabývá v teoretické části podnikovými informačními systémy, jejich zaváděními do podniků, bezpečností a outsourcingem. V praktické části se věnuje IS/IT Edscha Tools a.s. a to z hlediska bezpečnosti a ochrany dat, využití IS organizace při plánování výroby a komunikace se zákazníkem, možnostmi rozšíření IS/IT pro zaměstnance a vedení firmy.

červen 2007

Poděkování

Za cenné rady, náměty a inspiraci

bych chtěl poděkovat

vedoucímu práce Ing. Pavlu Pokornému, vedoucímu IT Ing. Lubošovi Kupkovi a vedoucímu výroby Jaroslavu Novákovi

OBSAH

ÚVOD

Tématem mé bakalářské práce jsou informační systémy a informační technologie v podniku. Vybral jsem si toto téma, protože mne při studiu bakalářského studijního programu zaujal předmět informační systémy organizací, kdy byl zpracováván podnik právě z pohledu těchto technologií. Při zpracovávání závěrečné semestrální práce pro tento předmět, mě informační systém v podniku Edscha Tools začal zajímat a proto jsem velmi uvítal možnost, zpracovat ho důkladněji.

Další věcí, která rozhodla o zpracovávání tohoto tématu, jsou kontakty, které ve firmě mám a věděl jsem tak, že mi budou poskytnuty informace, které budu potřebovat.

Cílem mé práce je tedy popsat zavádění informačních systémů do podniku, upozornit na věci, které se nesmí opomenout. Zmínil bych rád možnosti outsourcingu z pohledu informačních systémů a bezpečnost, která je velmi důležitá.

V praktické části, bych se chtěl věnovat popisu informačního systému, který podnik využívá a naznačit možnosti, které by vedly k rozšíření. Zajímat bych se také chtěl o jeho bezpečnost a zabezpečení proti útokům.

1 PODNIKOVÝ INFORMAČNÍ SYSTÉM (PIS)

„Podnikový informační systém vytvářejí lidé, kteří prostřednictvím dostupných technologických prostředků a stanovené metodologie zpracovávají podniková data a vytvářejí z nich informační a znalostní bázi organizace sloužící k řízení podnikových procesů, manažerskému rozhodování a správě podnikové agendy.“ [1]

1.1 Co jsou podnikové informační systémy

Jak je patrno z výše uvedené definice, nezdůrazňuje se tu potřeba hardwaru a softwaru. Ale důraz je kladen na činnost člověka, při vytváření informačního systému (IS) a jeho aplikaci do praxe. Právě přílišná orientace na softwarové aplikace a určité automatizace vede k neúspěchu zavádění informačních systémů do firem.

Různé organizace používají různé typy aplikací pro různé činnosti, v závislosti na potřebách, velikosti organizace a na finančních možnostech. Jednotlivé podniky mají specifické požadavky a svým způsobem unikátní podnikové procesy.

Informační systém by měl plnit integrační funkci podnikových procesů, tzn. pro různé úrovně vedení a pro různé úseky organizace by měly být přesně specifikovány požadavky na podnikovou aplikaci, která by měla plnit zadané požadavky. Nemělo by být zapomenuto na zabezpečení informačních toků směrem k zákazníkům a dodavatelům.

Je nutno zavést pořádek do každodenní agendy firmy, je tedy nutno jednotlivé informační kanály zpracovávat a informace z nich vyhodnocovat, za pomocí informačního systému. IS by měl na nepořádek v informacích upozornit a dohlédnout na odstranění chyby.

Všechny tyto informace, které systém zpracovává, by měly být následně využity pro manažerské rozhodování. Je tedy nutnost manažerů umět se systémem pracovat a využívat jeho možností, které usnadní každodenní práci a povedou k odstranění problémů při chodu organizace.

1.2 PIS a konkurenceschopnost

Konkurenceschopnost firmy je jedna z hlavních činností manažerů, ti musí zvažovat všechny okolnosti, které by mohly ovlivnit oblast podnikání, ve kterém se jejich firma nachází.

K zjištění těchto ovlivňujících okolností je možnost využít PIS a možné hrozby pomocí něj eliminovat.

Není-li v oblasti podnikání ještě poptávka po výrobcích a službách nasycena, hrozí vstup konkurenční firmy na trh. Z toho vyplývá nabídka produktů nebo služeb již trh po vstupu nové firmy nasytí a pravděpodobně vznikne převis nabídky nad poptávkou.

PIS může pomoci vstupu firmy na nový trh tím, že umožní jednotlivé kroky pohlídat a naplánovat, aby se firma mohla rovnocenně postavit tržním konkurentům. PIS umožní výrobním podnikům zabezpečit zkrácení termínu dodávek využitím plné kapacity výroby a tím pomůže řídit kritické zakázky klíčových klientů.

Na podnikatelském trhu může dojít k situaci, kdy zde působí v monopolním postavení společnost (monopolní zákazník), která si toho je vědoma a využívá toho při jednání s firmou a tlačí firmu ke snižování jejího zisku. Pokud na trhu působí konkurence, dostává se firma do problémů, kdy se bojí přijít o strategického zákazníka, ale zároveň nechce snižovat svůj zisk. PIS zde pomůže v oblasti prodejní logistiky, zlepšení rozmanitosti produktů a může pomoci při hledání nových zákazníků.

1.3 Vytváření podnikového informačního systému

Budovat informační systém nelze bez potřebných znalostí vztahů uvnitř organizace, bez znalosti strategických cílů a návazných podnikových činností. Je nutno mít přehled o vztazích k dodavatelům a zákazníkům a firma musí mít jasnou koncepci a strategii.

Teprve po splnění těchto dílčích kriterií je možno stanovit požadavky organizace na informační systém a začít s jeho budováním. Je nutno pečlivě zvážit, jaké přínosy očekáváme od jeho zavedení, zanalyzovat metody návrhu. Podnik musí také přijmout určité kompromisy, které zavedení přináší, není možné ve všech věcech přizpůsobovat pouze IS.

Bez těchto jasně stanovených kriterií je zavedení IS velmi riskantní a mohlo by dojít k nežádoucím překvapením při následném zavedení. Je to podobné jako by člověk stavěl dům, obstaral by jednotlivé části, ale nepřihlédl by k účelu stavby, okolní krajině, okolním domům, jeho využití apod. Těžko je pak možné dodržet stanový rozpočet, návrh architekta, či časovou rozvrženost stavby. Toto většina lidí při stavbě domů chápe, ale bohužel nepřihlíží již k tomu při zavádění PIS.

Často se pak stává, že určitá nekoncepčnost projektu firmě přináší nadměrné finanční výdaje a přínos je oproti tomu mizivý. Takže ve finální podobě IS firmu připravuje o možnost dalšího rozvoje a vysoké výdaje se odrážejí negativně na hospodářském výsledku společnosti.

1.4 Jednotný podnikový informační systém – nedosažitelný ideál

Nejčastěji chce managament při budování nového IS anebo při změně stávajícího IS zavést jediný komplexní, výkonný a efektivní systém.

Spousta firem při svém zahájení výroby nemá dostatek finančních prostředků na nákup nového uceleného systému, které zajistí všechny oblasti výroby a distribuce. Nakupuje proto jen jednotlivé části, které zrovna potřebuje. Při nákupu dalších částí systému si např. vybírá jinou firmu, než která dodávala předchozí část a tím vzniká problém kompatibilnosti systému a z toho vyplývající následné problémy, které spočívají v tom, že nedochází k očekávané efektivitě, výkonnosti a ke snižování nákladů. Firma, která již nějaký stávající systém využívá, si většinou slibuje, že zmizí určitá roztříštěnost a nesourodost stávajícího IS.

Na druhé straně ovšem stojí požadavky firmy, které nedokáže poskytovatel služeb naplnit, a to proto, že je jednoduše nenabízí. V tomto případě je nutno se obrátit na jinou firmu, pro kterou nebude problém novou službu do stávajícího systému zavést.

1.5 Ekonomika přínosů a nákladů

Informační systémy jsou nezbytnou součástí dobrého fungování podniku a jeho možnostech rozvoje. Proto si firmy uvědomují, že bez jeho pomoci není možné na trhu uspět. Vynakládají proto nemalé finanční prostředky na jeho zřízení a rozšiřování.
Předpokládají především tyto 4 přínosy:

1. vyšší efektivitu práce a chod celé společnosti – jedná se především o zkrácení času potřebného k provedení určité činnosti např. rychlost objednávky, rychlost kontaktu se zákazníkem a další. Vylepšení by se mělo týkat především oblastí systému logistiky, distribuční části logistického řetězce, podpory nákupu nebo-by se mělo zaměřit na systém účetnictví,

2. vyšší výkonnost – tímto termínem se myslí dosahování lepších výsledků (jak pracovních, tak i ekonomických) při stejném množství zdrojů. Jedná se o zlepšení řízení vztahů se zákazníky (CRM-Customer Relationship Management) pro podporu prodeje,

3. snížení nákladů – a tím pádem snaha o dosažení lepšího hospodářského výsledku firmy,

4. získáni konkurenční výhody před ostatními firmami a tím pádem větší možnosti získání nového zákazníka (internetové průzkumy, nástroje konkurenčního zpravodajství.

Je třeba říci, že firmy často kladou na systémy takové nároky, že není možno je splnit. Jednotný informační systém je tedy nedosažitelný ideál, ke kterému se ale firmy zabývající se zaváděním informačních technologií (IT - Information Technology) do podniků, snaží co nejvíce přiblížit.

První věcí, kterou podnik zjišťuje a analyzuje při rozhodování o investicích na nákup nových informačních technologií a nových informačních systému je, jestli přínos nově zavedených technologií bude větší, než celkové náklady na vlastnictví, kam patří investice a celkové náklady včetně nákladů interních.

Většinou bývá velmi složité vyčíslit přínosy IT. Existují sice metodiky, které toto dovolují, ale náklady na ně jsou velmi vysoké. Problémem je také zavedení sady ukazatelů výsledků a výkonnosti. Podniky jsou tedy spíše závislé na svých zkušenostech a znalostech ve svém podniku nebo podniků ve svém okolí.

1.6 Zákazník vs. Dodavatel

Podnik se snaží minimalizovat riziko tím, že nebude závislý na jednom dodavateli či providerovi služeb.

Je tedy snaha o určitou optimální úroveň vztahu zákazník – dodavatel. Problém nevzniká v poskytování primárních technologií, jakými jsou např. osobní počítač, server, síťové toky dat nebo ostatní počítačové komponenty. Tyto věci není problém nahradit jinými, na trhu je spousta výrobců těchto komponent a nabízejí v zásadě stejné produkty, které se liší jen nepatrně. Nejdůležitější oblastí v informatice jsou dnes data a datové informace, v našem

případě podniková data. Proto je tedy správný výběr dodavatele podnikových aplikací a podnikových technologií zásadní a mělo by být k tomuto faktu managementem přihlíženo při výběru dodavatele těchto služeb. Podnik by měl čerpat ze zkušeností ostatních firem, z recenzí a článků, kterých je nespočet. Je nutné také oslovit více firem a vybrat si ten produkt, který firmě bude nejvíce vyhovovat, a který přinese očekávaná zlepšení.

Po zavedení je nutno zvolit správu tohoto systému. Podnik má na výběr 2 možnosti. První je zabezpečení provozu interními pracovníky. Druhou možností je jistá forma outsourcingu. Je doporučována druhá možnost, která přináší jistou spolehlivost provozu, za který zodpovídá dodavatelská firma. Jistou nevýhodu představuje určitá závislost na této firmě, kterou lze jen těžko ovlivňovat a řídit. Dalším negativem je zneužití informací ze systému. Je nutno ošetřit tyto věci ve zřizovacích smlouvách.

2 ZÁKLADNÍ PRAVIDLA PRO ZAVEDENÍ CELOLOPODNIKOVÉHO INFORMAČNÍHO SYSTÉMU A JEJICH ÚSKALÍ

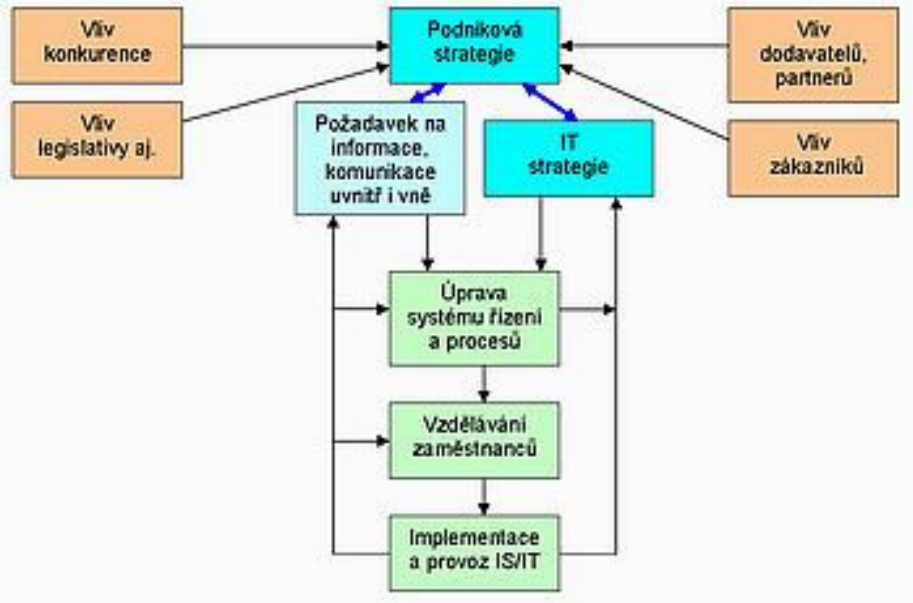
„Řada firem podceňuje dopad zavádění informačního systému do firemních procesů, hodnotí pouze to, jak nový informační systém nahradí stávající zastaralý, zajímají se pouze o jeho funkcionalitu a v nejhorším případě jen o cenu. Existují firmy, které se nedívají do budoucna, věří své intuici a subjektivnímu dojmu.“ [12]

Management firmy zapomíná zhodnotit dodavatele, zjistit si podrobné reference a vývojové a servisní zázemí firmy. Tyto nedostatky často ústí v předčasné ukončení celého projektu. Proto je nutné tyto nedostatky ve firmách odstraňovat a management by se měl této problematice hlouběji věnovat a nepodceňovat tyto situace, které pak vedou ke zbytečným finančním nákladům firmy a nulovému přínosu.

2.1 Problémové oblasti zavádění informačního systému

Při zavádění komplexního informačního řešení je nezbytně nutné věnovat se následujícím oblastem:

1. Je nutné si ve firmě, mezi vrcholovým managementem, ale také zaměstnanci, stanovit jasné strategie a cíle. Myslí se tím především stanovení toho, co od systému očekáváme. Nedostačující je, zvolit si pouze, že chceme zlepšit ekonomickou situaci a že IS bude používat pouze finanční oddělení společnosti na vedení účetnictví a další finanční agendy. K takto stanovenému cíli by stačilo zadat jen účetnictví nějaké externí firmě, která by nám ho zpracovala. Je nutný podrobnější přístup, který nebude pouze a jenom v obecné rovině. Otázky jako např. Kam firma chce směřovat? Které trhy chce obsáhnout? Čeho na nich chce dosáhnout? Které prostředky k tomu potřebuje? Musí být zodpovězeny velice podrobně,



Obrázek 1: Zavádění outsourcingu

Zdroj: http://casopis.systemonline.cz/292-uskali-zavadeni-is-it-ve-firme.htm

2. Dalším bodem je tok informací ve firmě. Analýza stavu, ve kterém se tok informací nachází, je dobrým předpokladem pro úspěšné fungování systému nového. Pod analýzou si představme efektivnost jednotlivých procesů, předávání informací jak v horizontální tak i vertikální struktuře a to jestli je předávání dostatečné. Dalším bodem analýzy je např. určité zpoždění předávání (prodleva) informací, která by mohla zapříčinit problémy rychlého a operativního jednání. Analýze by měl podléhat také stávající software – jeho aktualizace, servis, rozšiřitelnost, spolehlivost, a zda vyhovuje společnosti. Není nutné všechen stávající software nahrazovat softwarem novým, je možné zjistit, zda by nebyl kompatibilní s novými aplikacemi, které chce firma zavést. V opačném případě, kdy by byl starý software nahrazen novým ve stejném rozsahu, jednalo by se o zbytečně vynaložené neefektivní investice,

3. Stav nynější hardwarové (počítačové sestavy, tiskárny, modemy, routery) a softwarové techniky (operační systém, kancelářské programy, vývojové a kreslící aplikace atd.) je nutné velmi důkladně před zavedením podnikové informační technologie zkontrolovat. Nedostatečná výkonnost stávající techniky může být velkým problémem, proto se vyplatí, je-li současná technika již zastaralá, jsou programy nestabilní a aplikace neočekávaně havarují, nakoupit nový hardware, který bude novému systému vyhovovat. U každého IS jsou uvedeny minimální konfigurační požadavky na hardware a software, tyto požadavky je při nákupu nutno sledovat. Ale

nakoupit hardwarové a softwarové vybavení pouze v minimální konfiguraci je velkou chybou. Vždy je nutno investovat více prostředků pro kvalitnější vybavení. Systém by nám jistě při tomto minimálním setupu fungoval, ale byl by pomalý s možností výskytu chyb a pomalému datovému toku z důvodů zahlcení systému. Při nákupu techniky je důležité uvědomit si, jestli budeme systém časem rozšiřovat, protože složitější systém opět přináší větší nároky na počítačové vybavení a my potřebujeme komunikovat s okolím na příslušné úrovní. Nezapomínejte rovněž na bezpečnost podnikových dat a sítě,

4. Je-li ve firmě dobrá vertikální komunikace, tj. komunikují-li spolu vedení a zaměstnanci, přistupují pracovníci ke změnám ve firmě aktivně. Jsou ochotni probírat s vedením připravované změny, aktivně do nich mluvit, navrhovat svoje řešení. Tento bod je při implementaci IT často pomíjen a management je pak překvapen negativním přístupem zaměstnanců k novým IS. Je dobré vydat v podniku samostatnou směrnici, která bude upravovat všechny činnosti, které souvisí se zaváděním PIS. Praxí je ověřeno, že zaměstnanci pak systém přijmou snáze, ve směrnici by mělo být i jasně stanovena motivační složka pro pracovníky, nejen ve formě finančního ohodnocení, ale i ve formě zlepšení pracovních podmínek na pracovišti a v podniku jako celku,

5. Vzdělávání zaměstnanců v oblasti IS/IT je nutnou podmínkou pro efektivní fungování celého informačního systému. Je nutno provést vstupní školení, kde se pracovník seznámí s jednotlivými částmi a intenzivně se proškolí jen s částí, se kterou bude pracovat. Je velkou chybu snažit se pracovníky naučit pracovat s celkovým systémem hned ze začátku. Celkové znalosti IS se docílí pouze dalšími školeními, pracovními poradami a semináři. Naučí-li se zaměstnanec pracovat se systémem efektivně a správně, bude přínos pro firmu značný, zkrátí se čas nutný na jednotlivé operace a jednotlivé činnosti a zlepší se i celková spolupráce se zákazníky,

6. Při zavádění IS/IT se stanoví vedoucí projektu, který dohlíží nad všemi kroky. Tato osoba je z vedení firmy a má odpovídající pravomoci, oficiální ale i přirozenou autoritu, schvaluje jednotlivé kroky a informuje vrcholový management.

2.2 Přínosy znalostí oblastí IS

Při dodržení výše uvedených šesti bodů, při přípravě podniku na implementaci celopodnikového informačního systému, firma dojde do bodu, kdy její pozice při vyjednávání s dodavatelskými subjekty, které poskytují informační systémy a informační technologie, bude velmi dobrá a bude tak možno klást si určité podmínky, které budou dodavatelské firmy plnit (tlak na cenu, na další rozšíření apod.)

Firma si bude muset stanovit objem finančních prostředků, který bude ochotna investovat. Po stanovení těchto finančních mezí si firma bude moci vybrat z několika variant, které jí budou nabídnuty a zvolit pro sebe tu nejlepší, která ji bude vyhovovat, jak z hlediska financí, tak i z hlediska funkčnosti.

Podnik si také bude moci vytipovat všechny firmy, které budou přicházet eventuálně k dispozici. Budou totiž přesně stanovena jednotlivá kriteria a požadavky, takže bude moci být vypsáno výběrové řízení, jímž oslovíme vybrané firmy, které na naše jasně stanovené požadavky budou reflektovat.

Další možností je vyžádání si cenových nabídek firem a podle našich kriterií si vybereme dodavatele služeb v oblasti informatiky.

V dnešní době je čím dál tím víc běžné, že si firmy najímají nezávislého odborného poradce, který firmám pomáhá při orientaci v prostředí IS/IT a firmám se snaží nezávisle a odborně poradit při výběru dodavatele PIS. Tento odborný poradce by měl být znalý oblasti informačních technologií a procesů a měl by mít už zkušenosti s podobnými firmami. Je tedy nutné výběr konkrétního poradce zvážit a zjistit si o něm podobné reference, aby pak jeho přínos nebyl spíše problémem.

„Kvalita nabídky je dána také kvalitou poptávky z naší strany.“ [12]

2.3 Kriteria výběru PIS

Je nutno tedy správně zvolit (nastavit) kriteria výběru PIS. Mezi základní kriteria pro posouzení dodavatel informačního systému patří:

1. Cena – při tomto kriteriu bychom se měli řídit pouze tehdy, jsou-li nabízeny kvalitativně a funkčně srovnatelné systémy. V opačném případě nás může stát nakoupení nejlevnějšího informačního systému velmi mnoho problémů. Proto řídit se pouze cenou je jeden z největších problémů českých firem. Mnoho firem je pak zklamáno z přínosů systému a je nutno investovat další nemalé finanční prostředky do jeho dalšího rozvoje. Tyto nedostatky pak firmu sami porážejí na dnešním konkurenčním trhu a způsobují jim nemalé komplikace, které jsou daleko větší než očekávané přínosy,

2. Tradice – firma, která již na trhu nějakou dobu působí, je schopná vyhovět lépe naším požadavkům,

3. Kvalita – produktů je prvořadá a měli bychom na to brát zřetel,

4. Zkušenost – firmy zavádějící PIS je velmi důležitá, má totiž za sebou již celou řadu zakázek a je schopná při výskytu problémů pružně reagovat. Má za sebou již podobné zakázky a tedy zavedení celého systému by mělo proběhnout rychle a plynule. Následný provoz by již měl být také více bezproblémový,

5. Vývojové a servisní zázemí firmy – i kdyby byl systém sebelepší, nemusí fungovat správně, nebude-li kvalitní zázemí firmy. V opačném případě se vyskytne problém implementace. Pracovníci, kteří mají se systémem pracovat, nebudou řádně vyškoleni a jejich práce se systémem nebude do jisté míry rutinní,

6. Upgrade – neboli aktualizace systému. Různé firmy nabízejí různé aktualizace a různé ceny těchto aktualizací. Firma by měla sledovat tyto ceny a řídit se jimi při výběru systému. Systém musí umět pružně reagovat na změny, které jsou ve firmě i vně firmy a těmto změnám se musí přizpůsobit. Informace o upgradu jsou relevantní na průběh 1 - 3 let od zavedení systému,

7. Služby – které jsou zahrnuté do servisní smlouvy. U některých je upgrade zadarmo v rámci služeb zákazníkům, u některých je zpoplatněn. Je tedy nutné si smlouvu důkladně prostudovat, aby pak nedocházelo k nečekaným problémům způsobených neznalostí,

8. Reference firmy – jsou velmi důležitým faktorem. Doporučuje se navštívit konkrétní referenční místa a zde si domluvit schůzky s uživateli. Firma by si také měla zjistit počet úspěšných zavedení u firem s obdobným zaměřením produkce. Tyto informace, které získáme, nám podají ucelený obrázek o zvažovaném informačním systému. Počty úspěšných zavedení a rozhovory s uživateli, kteří již systém používají, jsou velmi užitečné a mohou nám tak podat částečný obrázek o tom, jak bude PIS fungovat v naší firmě.

3 OUTSOURCING

Outsourcing IS je dnes jedním z nejvíce diskutovaných témat v IT a současně i jedno z nejvíce polemických témat, ke kterému existuje tisíce názorů a stanovisek**.**

Co to vůbec tzv. outsourcing IT je? Outsourcing znamená přenést odpovědnost za dílčí činnost na externího poskytovatele služby, poskytovatele outsourcingu. Outsourcing IT je přenesení odpovědnosti za provoz, údržbu a vývoj systému na poskytovatele. Díky přenesení odpovědnosti se klient může věnovat předmětu své činnosti v plné míře a za péči o informační systém je zodpovědná externí firma.

Firmy většinou využívají vlastního IT oddělení. Ale vzhledem k rostoucí velikosti firem se postupem času ukáže tento způsob jako zcela neefektivní. Náklady na provoz už firmě nepřinášejí takový přínos, jaký by jim mohl za nižší cenu poskytnout externí dodavatel, pro něhož je tato činnost hlavním předmětem podnikání. Problém není pouze v mzdových nákladech na pracovníky, ale problémem se stávají náklady, které jsou spojeny s rozvojem znalostí, které pracovníci IT oddělení potřebují, aby mohli držet krok se stále novými a rozvíjejícími se technologiemi.

Společnost, která se outsourcingem zabývá, dokáže vedle běžné hardwarové údržby, jako je oprava a správa počítačových sestav a komponentů, inovace a optimalizace těchto sestav a jejich případná obnova zajistit i správu uživatelských kont a skupin, správu uživatelských login skriptů, zálohování dat, správu sdílených adresářů a souborů, antivirovou ochranu dat, správu systému elektronické pošty, konzultace v oblasti rozvoje informačních a komunikačních technologií (ICT - hardwarové a softwarové prostředky pro sběr, přenos, ukládání, zpracování, distribuci a zabezpečení dat) prostředí společnosti, instalace softwarového a hardwarového vybavení.

3.1 Důvody pro zavedení outsourcingu

Nejprve je nutné jasně si stanovit, co od zavedení outsourcingu čekáme. Zákazníci, kteří ho chtějí zavést, se zabývají především otázkou finančních nákladů a přínosů a s nimi spojených cen. Chtějí také mít jasnou definici a měřitelnost předávaných služeb, tedy kvalitu. Další oblastí je škálovatelnost služeb a sdílení rizik.

Mezi výše zmíněná kriteria můžeme zařadit i další, jako jsou stabilita poskytovatele, rozvoj know-how, inovační potenciál, technologie, podniková kultura, schopnost reakce na změny, kompetentnost, zlepšování finančních a nefinančních ukazatelů firmy.

Tyto kriteria mají pro různé zájemce různou váhu, tedy každá společnost nebo podnik přikládá různou důležitost různým kriteriím. I když se důležitost parametrů různí, jsou mezi sebou vzájemně propojena, z čehož vyplývá, že zlepšení v jedné oblasti může znamenat zhoršení v oblasti jiné. Toto je možné promítnout např. do stanovení kalkulace ceny a sdílení rizik. Dodavatel stanoví cenu, do které je nutné započítat i rizika, která vyplývají se smlouvy, tzn., že cena zakázky stoupne s ohledem na vyšší riziko.

3.2 Finanční náklady

"Mnoho firem tomuto bodu přikládá nejdůležitější váhu a první co ji zajímá je: O kolik bude levnější použití outsourcingu oproti provozování IT vlastními zdroji. Od této první věty se odvíjí celá řada dalších otázek, např. Jaké služby se dnes poskytují? Jaká je jejich kvalita? Co se stane, když se služba nedodá v požadované kvalitě, jaké to má dopady na organizaci? Co se stane, když budu chtít dodat větší nebo menší množství od dané služby, jakým způsobem se to promítne do ceny? Jak je zajištěn budoucí rozvoj interního IT firmy?" [2]

Na tyto otázky nejsou snadné odpovědi a je nutné tedy další analýzy.

Při stanovování ceny outsourcingu máme k dispozici 3 možnosti (hlavní přístupy) a to nákladový, výnosový a tržní.

Nákladový způsob není optimální pro zákazníka ani pro poskytovatele, přesto je ale nejobvyklejším způsobem při zavádění. Výhodou je, že se zákazník i poskytoval, mohou co nejlépe dohodnout. Je možné vycházet z údajů z dřívějších období a stanovit tak určitý vývoj pro období následující. Tento způsob spočívá v tom, že se každé jednotlivé činnosti přiřadí odpovídající náklady. Při těchto výpočtech je důležité nezapomenout na odpočet nákladů související se snížením počtu pracovníku provozující PIS.

Výnosový způsob stanovování ceny je obdobný. Tento způsob se snaží přiřadit jednotlivým činnostem skutečný podíl na zisku organizace. Tento způsob se ale moc nepoužívá, protože se nemůže říci, že IT poskytnuté v požadované kvalitě a množství nemusejí sami o sobě zajistit dosažení plánovaného zisku.

Tržní metoda stanovování ceny by měla být podle způsobu, kterým se stanovuje nejjednodušší, protože vychází z porovnávání ceny jednotlivých dodavatelů služeb. Ale ve skutečnosti je právě tento způsob nejvíce problematický. Velmi těžko se totiž porovnávají jednotlivé služby, ne vždy jsou totiž identické a ne vždy jsou nabízeny ve stejném rozsahu. Vytváření outsourcingového vztahu je velmi dlouhým procesem mezi zákazníkem a dodavatelem. Není ho tudíž možno vytvořit během několikaměsíčního výběrového řízení.

Do tohoto bodu, tedy do finančních nákladů, můžeme také zařadit další ukazatele jako je počet zaměstnanců, efektivita produkce a práce, zisk, hospodářský výsledek a další. U těchto ukazatelů je pouze potřeba vybrat ty správné, ty které jsou pro firmu směrodatné, protože se mění výrazně podle druhu organizace.

3.3 Definice a měřitelnost služeb

Aby nám z dlouhodobého hlediska přinášely služby trvalé úspory, je nutno náklady přesně rozpočítat na jednotlivé pracovníky, procesy nebo výrobní oddělení, které je spotřebovávají. Definujeme-li přesně jednotlivé služby, poskytuje nám tato definice informaci o tom, jestli tuto službu opravdu potřebujeme nebo naopak nepotřebujeme a zda jsme ochotni za tuto službu zaplatit stanovenou cenu. K tomuto určení nám slouží SLA[1] (Service Level Agreement). Pokud není jasná vazba mezi IT a jednotlivými procesy, je velmi těžké náklady na ně snižovat. Jsou totiž velmi často rozpuštěny v režijních nákladech. Ke snížení je tak možno dojít pouze pomocí administrativních příkazů.

3.4 Škálovatelnost

Mezi velké přínosy outsourcingu se také řadí škálovatelnost. Ta je možná pouze tehdy, nemá-li poskytovatel pouze jednoho zákazníka, ale má-li zákazníků víc. Škálovatelnost nám umožní dosahování synergických efektů. Úspory jsou vytvářeny hlavně sdílením provozní a bezpečnostní infrastruktury, vývojových a testovacích zařízení, zálohovacích systémů a prostředků pro zajištění provozu po živelné katastrofě (disaster recovery).

---

[1] http://www.totalservice.cz/solutions_cz.php?menu=188

Velkou roli hraje v dnešním světě IT know-how pracovníků, které je podmíněno stále lepšími a intenzivnějšími školeními a semináři. Školení externisty jsou kvalitnější, protože firma nemůže mít takové odborníky, ale zase jsou drahá, takže jednoduché věci si školí firma sama, složité za nemalé peníze u externistů.

Pro fungování a zajištění poskytování služeb 24 hodin denně po 365 dní v roce klade velké nároky na dostatečné množství kvalifikovaných pracovníků. Zabezpečení takového provozu je velmi náročné na pracovní kapacity. Při dobrém fungování uceleného systému není pro externí dodavatele a jejich zaměstnance pokrytí takového provozu zas až tak náročné. Při správně vybudovaném systému není totiž pro operátora rozhodující, zda se stará o jeden nebo více fungujících systémů. Pro outsourcingovou firmu je ale velmi nákladné zajistit nepřetržitý provoz pro jednoho zákazníka. Je nutné tedy využívat synergického efektu a z něj vyplývajících úspor z rozsahu. Zároveň ale není možné, aby synergický efekt byl zneužíván a jeden operátor by se staral o velké množství firem. Potom by úroveň poskytovaných služeb již nebyla na špičkové úrovni a zákazník by to jistě brzy poznal. Současné výpočetní systémy sice toto umožňují, ale smlouvy outsourcingových firem se zákazníky takto postavené nejsou. Problém je v určitých špičkách, kdy jsou na podnikový informační systém kladeny zvýšené nároky. Jedná se u většiny firem o stejný časový horizont a to o konec měsíce, čtvrtletí, roku. Výkon systému a jemu odpovídající personální zabezpečení musí být stanoveno na tuto špičku a jasně definován parametr v SLA.

Poskytoval outsourcingových služeb si musí tedy vybudovat kvalitní infrastrukturu včetně dohledových středisek. Pokud se mu toto podaří je schopen rychle a kvalitně reagovat na problémy v systému a poskytovat tak komplexní služby za výhodnější ceny než konkurence.

3.5 Sdílení rizik

Při uzavírání smlouvy mezi dodavatelem outsourcingových služeb a zákazníkem je nutno sdílení rizik velmi přesně definovat (kdo za rizika odpovídá, kdo nese náklady, jak rychle musejí být problémy vyřešeny atd.).

S rozdělením rizik je velmi úzce propojeno stanovení konečné ceny za poskytování služeb. Pro informační systémy a technologie je typické, že dopad na firmu z hlediska nefunkčnosti systému není lineární a velmi se liší, tím se liší také cenové dopady na firmu. Je velkým problémem, když při nefunkčnosti systému např. nemohou do skladu ani ze skladu proudit

vozy se skladovými položkami a konečnými výrobky nebo není možno obsloužit zákazníka čekající ve frontě nebo není možné vytisknout faktury, poslat objednávky atd. Na druhé straně existuje spousta činností firmy, na které výpadek PIS nemá žádný vliv a nepřináší firmě žádné ekonomické ztráty popř. odliv zákazníků.

Velký problém nastává pro každou firmu při dlouhodobějším výpadu v řádu několika dnů. Tento stav může být pro podnik velmi kritický a může mu způsobit dalekosáhlé následky a to nejen finanční. Při zavedení PIS jsou všechny činnosti na tento systém úzce vázány a jeho výpadek zapříčiní velké problémy.

Náklady související s rizikem se velmi promítají do konečné ceny a mohou ji značně navýšit. Pro výpočet tohoto navýšení se může vycházet z pravděpodobnosti poruchy a velikosti dopadu nebo poskytovatel hradí část ušlých příjmů. Tyto podmínky je nutno ve smlouvě velmi přesně specifikovat. Zákazník si musí sám zvážit jaká rizika je ochoten nést a za jaká už přenechat odpovědnost jiným a kolik je ochoten za toho přenesení zaplatit.

3.6 Důvěra v outsourcingu

Všechny doposud zmíněné faktory jsou víceméně měřitelné a zjistitelné. Důvěra mezi poskytovatelem služeb a zákazníkem se měřit nedá, ale její role je více než důležitá.

Toto kriterium může významně posílit nebo naopak převážit nad ostatními 4 faktory. Vyjmutí IT mimo vlastní organizaci je dlouhodobý proces, který musí být přesně naplánován. Není možné na něm zkoušet nějaké pokusy či nejisté kroky. Firma si musí být stoprocentně jistá, že činí správné rozhodnutí, když najme outsourcingovou firmu. Tato důvěra nevznikne pouhým podepsáním smlouvy, ale dlouhou a intenzivní spoluprácí na různých projektech a zadáních, při řešení běžných činností a vyskytujících se problémů.

3.7 Nedůvěra k outsourcingu je velmi drahá

„Velké evropské podniky přicházejí o potenciální úspory ve výši 5,4 miliardy liber ročně, protože se bojí svěřit některé činnosti externím dodavatelům formou outsourcingu. V současné době činí tyto úspory asi 2,2 miliardy liber, což ukazuje, že se zdaleka nejedná o vyspělý trh, a to nejen ve srovnání s ideálním stavem, ale také v porovnání s pokročilejšími trhy. Uvádí se to v analýze, kterou zveřejnila společnost LogicaCMG.“ [13]

Podle této analýzy se optimální rovnováha mezi zajišťováním činnosti vlastními zaměstnanci a pronájmem služby od externího dodavatele pohybuje kolem poměru 30:70. To znamená, že by společnost měla realizovat vlastními silami přibližně třetinu svých aktivit. Tento poměr se ale může v jednotlivých zemích lišit podle pracovních zákonů, které toto omezují. Studie také ukazuje, že dobré outsourcingové kontrakty mohou výrazně snížit nejrůznější podnikatelská rizika. V této souvislosti je zarážející, že téměř 60 % velkých evropských podniků se analýzou rizik nezabývá vůbec a mnoho dalších firem až v situaci, kdy začínají uvažovat o outsourcingu činností. Rizika spojená s provozováním činností vlastními silami tak zůstávají skryta.

Základem výzkumu byly hloubkové pohovory s přibližně dvěma stovkami vrcholových manažerů největších společností ve Velké Británii, Francii, Německu, Nizozemí, Belgii a Austrálii, které provedla nezávislá agentura Coleman Parkers. Co se týče odvětví, byly do výzkumu zahrnuty veřejná správa, finance, doprava, telekomunikace, energetika a výrobní průmysl. Dotazováni byli nejčastěji provozní ředitelé, členové představenstev odpovědní za provozní záležitosti a finanční ředitelé.

Z průzkumu vyplynula zjištění, že: 78 % společností (97 % firem ve Velké Británii, 71 % v Německu a 70 % ve Francii) se nějak zabývá analýzou rizik, ale mnoho z nich není schopno vidět rizika spojená s procesy, jež probíhají přímo uvnitř organizace. Nejčastěji uváděné důvody proti outsourcingu jsou tyto: jedná se o činnost příliš důležitou (40 % dotazovaných firem), jedná se o činnost blízkou hlavnímu podnikání, kde je přidáváno hodně hodnoty, a tak je těžké zdůvodnit předání takové činnosti někomu jinému (42 % firem) a náklady (7 % firem).

Francouzské společnosti spojují s outsourcingem očekávání největších úspor (22 %), zatímco britské společnosti jen 16 %.

	UK (%)	France (%)	Germany (%)	Belgium (%)	Netherlands (%)
Účetnictví	20	3	6	0	7
Personální agenda	13	3	3	8	3
Informační technologie	43	33	13	35	10
Řízení řetězce dodávky	20	3	19	13	17
Vývoj a inovace	27	3	3	3	13
Mzdová agenda	40»	13	6	50	50

Tabulka 1: Úroveň částečného nebo úplného outsourcingu jednotlivých typů činností

Zdroj: http://www.systemonline.cz/clanky/neduvera-k-outsourcingu-je-draha.htm

Přínos	Průměr všech zemí
Snížení nákladů	3,9
Lepší úroveň služeb	3,7
Možnost předvídat náklady	3,6
Zlepšení výkonnosti organizace	3,5
Zlepšení řízení procesů	3,4
Rozšíření kapacity zpracování dokumentů, požadavků atd.	3,3
Možnost lépe využít vnitřní zdroje	3,3
Zlepšená reputace na trhu	3,2
Konkurenční výhoda	3,2
Snížení podnikatelského rizika	2,7

Tabulka 2: Co společnosti očekávají od outsourcingu (1-bezvýznamné, 5-velice důležité)

Zdroj: http://www.systemonline.cz/clanky/neduvera-k-outsourcingu-je-draha.htm

4 NEBEZPEČÍ OHROŽUJÍCÍ BEZPEČNOST PIS

Při řešení bezpečnosti v IS se setkáváme s velkou škálou názvů a pojmů. Bude nutné si je osvětlit a zobecnit.

Obrázek 2: Základní bezpečností pojmy a vztahy mezi nimi

Zdroj: Hanáček, P., Staudek, J.: Bezpečnost informačních systémů, ÚSIS, Praha, 2000

4.1 Aktiva

Tvoří souhrn technologií, aplikací, dat a také osob. Mezi data je tedy možno zařadit veškeré technické prostředky, software a data, která jsou v podniku v oběhu, a která jsou využívána. Nesmíme opomenout také pracovníky, kteří pracují jako správci aplikací, komunikace a řadí se sem také všichni pracovníci oddělení informatiky.

Aktivum je tedy všechno co má pro každého jednotlivce určitou hodnotu. Tato hodnota může být do jisté míry zmenšena působením hrozby.

4.2 Zranitelné místo

Tímto termínem je nazýváno místo v IS, kde je určitá slabina, která může být využita ke způsobení škod nebo ztrát útokem.

Existence zranitelného místa je důsledkem chyby v analýze. Toto místo může také vzniknout díky velké složitosti systému, vysoké hustoty uložení informací apod.

Příčina zranitelného místa může být:

1. Fyzická – jedná se především o umístění IS v místě, kde je snadný přistup pro sabotáž, vandalismus a může zde dojít k jeho poškození, ztrátě či zničení,
2. Přírodní – kdy prvek nemá možnost se vyrovnat s některými objektivními faktory typu vichřice, uragán, záplava, zemětřesení, blesk,
3. V hardwaru nebo softwaru – kdy prvek IS není sto schopen zajistit plynulý a trvalý provoz,
4. Fyzikální – kdy prvek pracuje na velmi vysokém fyzikálním principu např. útoky při komunikaci na výměnu zprávy,
5. Lidská – tato možnost je největší zranitelnost ze všech možných. Místa vznikají v důsledku lidského faktoru jako je opomenutí, neznalost, omyl, úmysl apod.

4.3 Hrozba

Pod tímto pojmem je nutno představit si možnost využít zranitelné místo IS k útoku na něj a tím ke způsobení škody na aktivech.

Útok označujeme jako bezpečnostní incident, což je vlastně kterákoliv událost, která vede k nedodržení pravidel IS/IT. Nemusí se jednat o porušení, stačí, když se o toto porušení někdo pokusí.

Hrozby lze rozdělit na:

1. Objektivní – kam patří hrozby přírodní a fyzické, fyzikální, technické a logické,
2. Subjektivní – což jsou hrozby plynoucí z lidské činnosti, ty je možno dále dělit na neúmyslné a úmyslné (lidé pracující uvnitř firmy nebo zde dříve pracovali. A v nadnárodních společnostech např. špioni nebo teroristé).

Pod charakteristikou hrozby je potřeba představit si zdroj, který může být vnější nebo vnitřní.

Typické hrozby pro IT v podniku neboli distribuované systémy jsou např. přeměna informací, kdy je změněn jejich obsah, odchytávání zpráv, kdy se zabraňuje přenosu zpráv k příjemci.

Často je také napadán systém tím, že jsou do něj vkládány špatné (podvržené) zprávy (fake). Patří sem také odposlechy, kopírování dat z paměťových míst.

V síťovém prostředí dochází také k četným útokům na systém IT. Podle posledních studií jsou to nejčastěji:

- Odposlech – kdy se jedná o útok v síti, jehož účelem je zcizení informace, jako je číslo kreditní karty, číslo účtu zákazníka. Znalost komunikace mezi dvěma podniky umožňuje třetí firmě získat konkurenční výhodu a tím se dopustí trestného činu,

- Vyhledávání hesel – tím, že neoprávněný útočník získá heslo, umožní se mu tím přístup do systému, dokáže tak získávat informace apod. K nejčastějším útokům se řadí využití trojského koně, který získá potřebné informace a uloží je tak, že jsou dostupné útočníkovi,

- Modifikace dat – je útokem, kdy se mění data a informace uložené v systému, třeba i počítačovými viry.

Útočníci často také používají speciálně vyvinuté programy, které mají za úkol poškodit soubory, data a zařízení nebo zcizit informace. Tyto programy se nazývají škodlivé kódy.

Řadíme mezi ně:

- Viry – název těchto útočníků je odvozen z biologických prvků v důsledku podobného chování. Počítačový virus je zvláštní forma útočníků, která se dokáže sama množit a dokáže se dostat do systému bez vědomí uživatele. Činnost virů nemusí být vždy škodlivá, jedná-li se např. o vtipy, reklamu. Většina z nich ale systémům škodí tím, že dokáže mazat obsah systému či data nebo ho záměrně poškozuje,

- Trojské koně – se do počítače dostávají pomocí nějakého programu. Kód takové programu má ve svém těle ukrytou část, která se aktivuje nějakým impulsem. Tento impuls může být např. určité datum, počet spuštění programu, počet spuštění počítače, počet kliknutí apod. Tím, že se kůň aktivuje, začíná jeho destruktivní charakter. Sám se ale oproti viru nedokáže replikovat,

- Červi – jsou sebereplikující, nepotřebují žádnou aktivaci a sami se množí, popř. rozesílají. Dokáží sami sebe replikovat,

- Hoax – poplašné zprávy šířící se e-mailem popř. ICQ, které upozorňují na libovolnou událost a počítají s tím, že bude předána dále,

- Spyware – kód, který je zaměřen na sledování počítače popř. systému a tyto data pak dokáže odesílat. A podmnožinou spyware je trojský kůň.

4.4 Útok

„Někdy bývá nazýván též jako bezpečnostní incident. V podstatě se jedná o využití zranitelného místa systému, kam útočník pronikne a snaží se způsobit ztráty na aktivech. Může se také jednat o neúmyslnou činnost, která poškodí aktiva IS.“ [3]

Je nutná včasná analýza útoků, při které je potřeba vyřešit otázky, např.: Jak se projevuje počítačová kriminalita? Jaké jsou možné formy útoků apod.

Následně je nutné, po zodpovězení otázek, rozhodnout o možném řešení útoků. Je nutno detekovat útok a zjistit bezpečností incident.

Jsou různé formy útoku:

1. Přerušením – při tomto útoku dochází k situaci, kdy se útočník snaží přerušit dostupnost např. ztráta, znepřístupnění, poškození aktiva, porucha periférie, vymazání programu, vymazání dat, porucha v operačním systému,

2. Odposlechem – dochází k situaci, kdy se agresor snaží útočit na aktiva, tím že ačkoliv nemá povolení, snaží se data získat např. okopírování programu či okopírování dat,

3. Změnou – při tomto průniku dochází k tomu, že jsou změněna uložená nebo přenášená data. Často se také stává, že jsou přidány určité funkce do programu.

4.5 Útočník

Útočníkem nemusí být pouze osoba z venku, která s firmou nemá co dočinění. Naopak nejčastější útoky na PIS hrozí firmám zevnitř, ať už se jedná o bývalé zaměstnance nebo zaměstnance současné. Podle útočníkovy síly rozlišujeme útoky na 3 stupně:

1. Slabá síla – zde hrozí nejmenší nebezpečí, protože útoky jsou vedeny naprostými amatéry, náhodnými útočníky, kteří při své běžné práci objeví zranitelná místa systému. Tyto útoky jsou často neúmyslné a spíše náhodné. Tito útočníci mají často

velmi slabé znalosti a primitivní vybavení. Ochrana před nimi je velmi jednoduchá, stačí přijmout slabá bezpečností opatření, která nejsou finančně náročná,

2. Střední síla – jedná se o hackery, jež se snaží dostat tam, kde nejsou autorizování a nemají zde povolení. Tito útočníci již mají dostatek znalostí a i lepší vybavení, ale jejich útoky jsou pořád ještě snadno zjistitelné a dá se proti nim dobře bránit. Proti těmto lidem jsou potřeba bezpečnostní opatření střední síly,

3. Velká síla – v tomto případě už se jedná o naprosté profesionály, kteří se nabouráváním do IS zabývají cíleně. Jsou o to nebezpečnější, že mají velmi dobré znalosti a zkušenosti v oblasti IS/IT, mají dostatek finančních prostředků a často i dostatek času na to, aby se mohli do systému dostat. Proti těmto hackerům, pirátům a teroristům jsou už nutná silná bezpečností opatření, které stojí nemalé finanční prostředky.

4.6 Riziko

Rizikem myslíme v tomto případě pravděpodobnost, že bude využito našeho zranitelného místa IS. Riziko představuje existence hrozby.

5 ZABEZPEČENÍ IS PROTI ÚTOKŮM

V této části své práce bych se chtěl zaměřit na možnosti a řešení pro bezpečné fungování podnikového informačního systému. Nejprve je potřeba zmínit, že neexistuje žádné optimalizované řešení, které by firmu chránilo proto všem bezpečnostním úskalím. Není také možné zmínit všechny prvky, které jsou při zabezpečování systému používány.

Podle vztahu, který je mezi protiopatřením a bezpečnostním nabourání systémů můžeme protiopatření dělit:

1. preventivní – kdy je prvotním účelem těchto zabezpečení snaha o minimalizaci rizik, která by teprve mohla vzniknout, a která by mohla systém poškodit popř. zneužít jeho informací,

2. dynamická – smyslem těchto opatření je zabránit již vzniklému bezpečnostnímu incidentu, aby se šířil dál a minimalizovat tak dopady, které tento incident může vyvolat,

3. následná – tyto opatření se snaží zmírnit dopady již proběhlého narušení.

Podle formy je možné protiopatření členit na:

1. administrativní – kdy se nastavují pravidla, která vedou k minimalizaci vzniků a průběhu incidentu. Jedná se především o vzdělávání a školení uživatelů, a stanovování způsobů archivace dat,

2. fyzická – zde jde o snahu fyzicky zajistit aktiva proti zneužití. Typickým příkladem je uzamykání počítačů, serverů popř. informačních medií v uzamykatelných místnostech, ostraha objektů a kontrola osob vstupujících do podniku, se snahou zamezení přístupu nepovolaných osob,

3. technologická – třetím bodem je technologické protiopatření, tedy hardwarové a softwarové zabezpečení aktiv. Jde především o šifrování důvěrných dat.

5.1 Vybudování bezpečnosti v oblasti IT

Při budování zabezpečení informačního systému je nutné nejprve si stanovit některé základní body.

Je nutné přesně určit to, co bude vyžadovat ochranu, které hardwarové nebo softwarové prostředky budeme chtít chránit. Není totiž vždy nutné zabezpečovat všechny prostředky stejnou intenzitou zabezpečení. Je zbytečné vynakládat stejné finanční prostředky na zabezpečení serveru oproti zabezpečení počítače, který slouží pouze pro tabulkové aplikace.

Dalším bodem je určení, proti jakým hrozbám bude ochrana budována. Jestli pouze proti ojedinělým útokům nebo proti zkušeným hackerům, máme-li důvěrné a tajné informace.

5.2 Celková bezpečnost IT

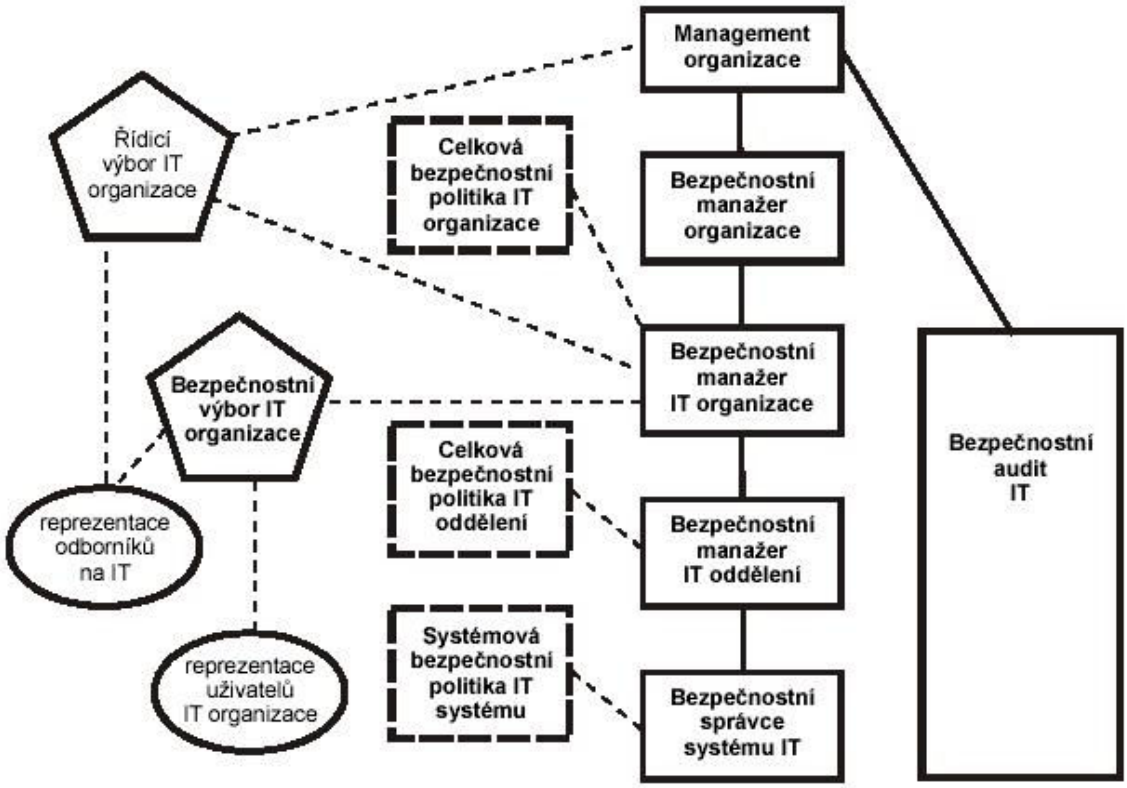
„Celková bezpečnostní politika IT uvádí specifikaci cílů zabezpečení, definici citlivých dat a klasifikaci těchto dat a definici ostatních citlivých aktiv IT a definici odpovědností za ně." [3]

Definuje bezpečnostní infrastrukturu organizace a potřebné síly mechanismů pro implementaci bezpečnostní funkčnosti. Specifikuje omezení, která musí bezpečnost IT organizace respektovat. Je vytvářena nezávisle na právě používaných informačních technologiích, a to v časovém horizontu obvykle pěti až deseti let.

Celková bezpečností politika je tedy veřejný závazný dokument, který je potřeba dodržovat.

Omezení, kterým organizace musí čelit, chce-li dodržovat bezpečnostní standardy, jsou závislá na prostředí, ve kterém se firma nachází. Mezi omezení se řadí především vyhlášky, standardy, zákony atd.

Celková bezpečnostní politika IT neobsahuje jména konkrétních lidí, produktů. To ale neznamená, že nejsou jasně stanoveny jednoznačné role, funkční místa a odpovědná pracoviště, že není stanoveno, kdo autorizuje přístupy, kdo odpovídá za plán činnosti apod.



Obrázek 3: Příklad bezpečnostní infrastruktury IT

Zdroj: Hanáček, P., Staudek, J.: Bezpečnost informačních systémů, ÚSIS, Praha, 2000

Bezpečnostní výbor řeší interdisciplinární problémy bezpečnosti IT a dává řídícímu výboru organizace strategické podněty. Dále zavádí bezpečnostní orgán a schvaluje administrativní opatření. Ne poslední činností je doporučování zdrojů (lidí, peněz).

Bezpečnostní manažer má jasně stanovený úkol spočívající v odpovědnosti za bezpečnost PIS v organizaci. Ze své funkce spolupracuje s bezpečnostním výborem a stará se o zavádění bezpečnostních programů.

Výkonným bezpečnostním orgánem je bezpečnostní správce, který spolupracuje s bezpečnostním manažerem, a který podléhá jeho řízení. Jeho činností je vyšetřování bezpečnostních incidentů.

Kontrolním orgánem je bezpečnostní auditor.

Je nutné říci, že toto schéma je využíváno u velkých firem, která mají složitá protiopatření proti ohrožování bezpečnostních jistot. U malých toto schéma také funguje, ale ve velmi zjednodušené podobě, kdy jeden člověk zastává více funkci.

6 HAVARIJNÍ PLÁN

Havarijní plán je důležitou součástí IS organizace. Je to systém kroků, který stanovuje, co dělat po odhalení útoku a jakými kroky postupovat, aby se udržel chod organizace a došlo k co nejmenšímu narušení. Pokusím se tedy popsat hlavní rysy plánu po bezpečnostním incidentu.

Havarijní plán určí místa, kde budou skladovány náhradní počítačové komponenty a jejich počet, určí místa, kde budou skladovány zálohy dat a způsoby, jak budou zálohovány, stanoví také obsah hardwarovým a softwarových komponent, určuje jak udržovat datové sklady, software a hardware aktuální.

Do havarijního plánu patří plán činnosti po útoku a také návod jak postupovat při obnově IS po havárii tzv. plán obnovy.

Havarijní plán se sestavuje a dolaďuje velmi dlouho, není to otázka čtrnácti dnů, ale často trvá jeho optimalizace i několik let. Tento plán se pořád vyvíjí, stejně jako se neustále vyvíjí IS a IT, není možné sestavit havarijní plán a v nezměněné podobě ho používat 10 let, kdy technologické vybavení bude už úplně jiné.

6.1 Plán činnosti po útoku

Plán činnosti po útoku je souborem kroků, který stanovuje jak postupovat po bezpečnostním incidentu, který se liší délkou přerušení činnosti, ztrátou vybavení, znemožnění přístupu do areálu organizace.

Dojde-li k incidentu, je nutno tento incident zanalyzovat a zdokumentovat pro další možné útoky. Dokumentace musí obsahovat podrobné údaje o tom, co se stalo, jaké vznikly škody, jak se postupovalo a co naopak bylo chybné. Po analýze a dokumentaci se přijímá závěr, zda bylo po útoku provedeno vše efektivně a správně, a kde byly ještě určité nedostatky, které je nutno pro příště odstranit a plán tak modifikovat.

6.2 Reakce na incident

Jakmile dojde k útoku na informační systém, je nutný zásah, který je stanoven plánem činnosti ve stavu nouze, což jsou návody jak postupovat, jsou zde telefonní čísla na kontaktní osoby nebo správce systému. Dochází k odhalení důsledků útoku a snaha o uvedení systému do původního stavu.

6.3 Plán obnovy

Plán obnovy musí obsahovat kriteria definující to, co se vůbec považuje za havárii, odpovědnost za aktivaci obnovy, odpovědnost za aktivaci dílčích činností.

V plánu obnovy je třeba rozlišit věci, které jsou pro organizaci a IS prioritní a těmi se zabývat nejdříve. Nejkritičtější zdroje je třeba obnovit do cca 30 minut, ostatní kritické zdroje do cca 2 hodin a zbývající zdroje do 24 hodin. Velmi důležité je, aby byla stanovena posloupnost kroků ve všech odděleních organizace. Toto je velmi nutné aby se systém vrátil do původního bezchybného stavu

7 ZÁKLADNÍ INFORMACE O FIRMĚ

Adresa:

Edscha Tools a.s.

Dolní Skrýchov 59

37781 Jindřichův Hradec

Telefon: +420 384 341 511

Telefax: +420 384 341 520

Internet: www.edscha.cz

E-Mail: jrathouska@edscha.cz

Kontaktní osoby:

Zákaznický servis

Stanislav Licehamr

Telefon: +420 724 424 522

E-Mail: SLicehamr@edscha.cz

Vedení závodu

Zdeněk Krofta

Telefon: +420 724 424 118

E-Mail: ZKrofta@edscha.cz

Vedení výroby

Jaroslav Novák

Telefon: +420 724 424 535

E-mail: JarNovak@edscha.cz

7.1 Představení společnosti

Edscha Tools a.s. sídlí v Jindřichově Hradci. Je úzce svázána s Edscha Bohemia, která sídlí v Kamenici nad Lipou, kde je veškerá administrativa a také nejvyšší vedeni společnosti. Vlastníkem akcií je Edscha AG se sídlem v Remscheidu (Německo). Edscha Tools má v konsorciu Edscha AG výjimečné postavení, neboť jako jediná z 24 částí se nezabývá výrobou pro automobilový průmysl. Má dlouholeté zkušenosti v konstrukci a výrobě speciálních nástrojů:

- lisovacích nástrojů včetně postupových,
- vstřikovacích forem a forem na tlakové lití.

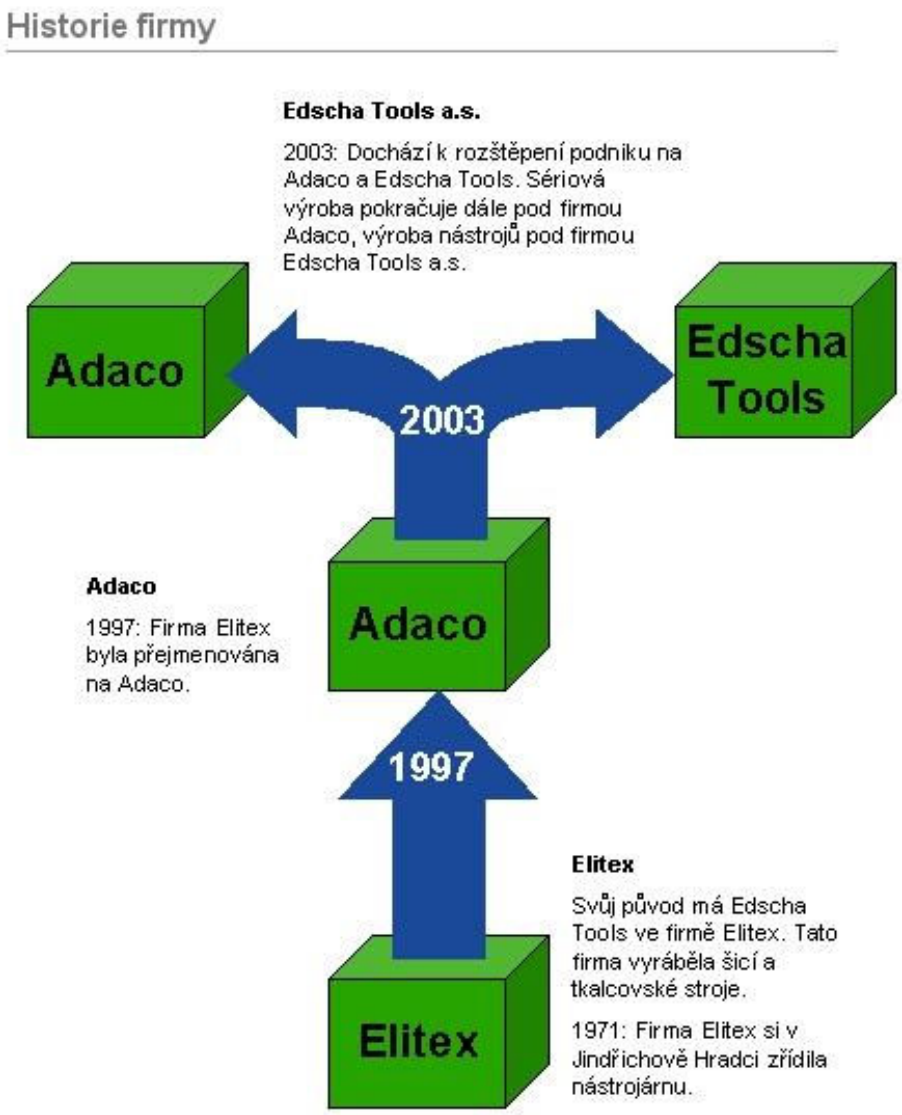
Obrázek 4:Tlakové odlitky[2]

V České republice patří k čelním výrobcům lisovacích forem. Jsou také schopni vyrábět postupové lisovací nástroje na plechy do tloušťky 6 mm. Jejím hlavním odběratelem je Edscha Grup. Dalšími odběrateli jsou např.:

- Klein & Blažek, CZ,
- Dr. Franke, D,
- Forma Gradu, CZ,
- Stanley, GB / USA.

V roce 2003/2004 dosáhla tato firma se svými 82 zaměstnanci ve dvousměnném provozu obratu přes 100.000.000 Kč. Tento výborný obchodní výsledek jim umožňuje dále investovat, do nových strojů, nových technologií, které povedou ke zlepšení konkurenceschopnosti firmy na trhu a k dalšímu růstu zisku.

[2] http://edscha.cz/ed_tools/CZ/index_CZ.htm



Obrázek 5:Historie firmy[3]

7.2 Produkty

- Formy pro tlakové odlitky z hliníku, magnézia a zinku - do hmotnosti 3.000 kg,
- Formy na zastříknuté a plastové díly - do hmotnosti 3.000 kg,
- Postupové lisovací nástroje pro automatizovanou výrobu,
- Drobné přípravky pro třískové obrábění (řezání, vrtání, frézování),

[3] http://edscha.cz/ed_tools/CZ/index_CZ.htm

- Svařovací přípravky,
- Lisovací nářadí.

7.3 Co firma nabízí

Edscha Tools se specializuje na výrobu speciálního řezacího a postupového nářadí, jakož i zástřikových forem a forem na tlakové lití dle zvláštních přání zákazníka. Díky kombinaci moderních a konvenčních technologií jsou schopni:

1. Zajistit nejvyšší kvalitu jejich produktů,
2. Nabídnout výhodné technologické řešení dodávky různého objemu,
3. Reagovat pružně na přání jejich zákazníků,
4. Dodržet krátkodobé dodací lhůty.

8 PLÁNOVÁNÍ VÝROBY A KOMUNIKACE SE ZÁKAZNÍKEM

Edscha Tools je informačním systémem úzce spjatá se svojí „mateřskou společností“ Edscha Bohemia, která sídlí v Kamenici nad Lipou. Zde se provádí veškerý dohled nad informačním systémem v Edscha Tools. Svoji kancelář zde má i vedoucí útvaru informačních technologií pan Ing. Luboš Kupka, který mi poskytl potřebné informace.

8.1 Informační systém LCS

Firma Edscha Tools využívá podnikový informační systém Helios Orange, dříve nazývaný Helios IQ, od firmy LCS, která je českou jedničkou na trhu s informačními a podnikovými systémy. Firma byla mnohokráte oceněna v prestižních soutěžích ERP Czech 2004 a Microsoft Industry Awards, což řadí produkt Helios Orange mezi špičkové produkty na informačních trzích.

“LCS Helios je unikátní řešení moderního, inteligentního, informačního systému dostupného středně velkým a menším firmám. Je snadno implementovatelný v podnicích zabývajících se výrobou, službami i obchodem. Systém je velmi kompatibilní a umožňuje integrovat nejen běžné kancelářské aplikace, ale propojit doposud používané systémy." [15]

Středně velké firmy jako je Edscha Tools a.s. oceňují především množství specializovaných oblastí a návazných řešení, které umožní pokrytí procesů ve firmě. Systém se dokáže přizpůsobit specifickým požadavkům.

Helios Orange pracuje na technologii client/server, na kterém je systém vystavěn. Výhodou této technologie je dostatečná stabilita a bezpečnost dat. Je zde použito výhradně MS SQL serveru, který zajišťuje maximální rychlost a neomezenou práci s uloženými daty.

Obrázek 6: Oblasti LCS

Zdroj: www.helios.eu

8.1.1 Fungování Helios Orange – modul výroba

Helios IQ je zde rozšířen o modul Výroba, zahrnující, jak technickou přípravu výroby, tak i kapacitní plánování a řízení výroby, včetně variantního řešení výrobků.

Jak tedy Helios funguje: Nejprve přichází určitá poptávka od zákazníka a začíná interní kolečko, kde se řeší kapacitní možnosti firmy, popř. zda je možné využít externí firmy, vypracuje se určitá nabídka, která se odesílá potenciálnímu zákazníkovi.

Akceptuje-li zákazník nabídku, je potřeba vypracovat konstrukční a technologický návrh výroby, zjistit stav zásob materiálu na skladě, popř. zajistit dodání materiálu od smluvních dodavatelů.

Poté jde zakázka do výroby. Následuje montáž, sklad, expedice, vypracování dodacích listů, způsoby plateb. Výrobek se odváží k zákazníkovi, kde jsou na řadě zkoušky, není-li zákazník spokojen, výrobek se odváží zpět a celý proces se opakuje až k dokonalé spokojenosti.

Modul Výroba dále firmě pomáhá při plánování využití pracovních strojů a následných zpětných kontrolách, kdy jsou kontrolovány využitelnosti strojů, pracovníků a jednotlivých středisek.

8.1.2 Modul Obchod

Firma používá vedle modulu Výroba, který je nejdůležitější i další pomocné moduly. Jedná se především o modul Obchod, který rozšiřuje jádro systému o další důležité funkce.

Firma pomocí Helios Orange má dokonalý přehled o svých odběratelích ale i dodavatelích. Dokáže zákazníkovi poskytnout dokonalou kalkulaci pro jeho požadavek, který se může operativně měnit a přepočítání nabídkových cen je velmi jednoduché a hlavně rychlé, což zákazník požaduje.

Modul Obchod je také nápomocen při optimalizaci zásob, kdy sleduje maximální a minimální stavy a dává pověřenému pracovníkovi informace, kdy je potřeba zboží objednávat, aby bylo včas k dispozici.

Velkou výhodu systému Helios spatřuji v tom, že se nemusí zavádět celý modul, ale jen jednotlivé části, které firma potřebuje, a které využije. Což snižuje cenu, ale také zbytečně nezatěžuje systém o další nepotřebné součásti.

8.1.3 Další moduly

Vedle těchto dvou hlavních jsou využívány ještě další aplikace jako, je modul Lidské zdroje, který se týká personalistiky, mezd apod.

Edscha má klienty ve spoustě cizích zemí. Využívá tedy celní aplikace, které dovoz a vývoz zboží usnadňují. Dále využívá účetní aplikace pro některé operace.

8.1.4 Cena systému Helios

Pro představu ceny základních modulů:

Jádro systému	2 800 Kč
Technická příprava výroby	12 800 Kč
Oběh zboží	6 800 Kč

Tyto ceny jsou pouze orientační. Firma Helios si účtuje ceny za jednotlivé moduly a za uživatele, kteří je budou využívat.

Celková cena systému Helios ve firmě Edscha Tools stála okolo 700 000 Kč.

8.1.5 Systémové požadavky na provoz systému

Doporučený desktopový operační systém (operační systém PC uživatele) je MS Windows NT 4.0 Workstation, MS Windows 2000 Professional a MS Windows XP Professional.

Doporučený operační systém serveru je MS Windows Server 2003, Windows 2000 Server, Windows NT 4.0 Server, případně MS Windows XP Professional.

Pro server je to MS SQL 2005 Server (verze podle provozovaného operačního systému) s nainstalovaným aktuálním service packem.

9 MOŽNOST ROZŠÍŘENÍ PRO VEDENÍ

Co se týká rozšíření stávajícího informačního systému, vidím jako největší omezení firmy v tom, že by se mělo jednat opět o nějaký modul Helios.

Výběr jiného dodavatel by sice byl možný, protože systémy jiných firem spolu mohou komunikovat, ale tento výběr je problematický. Největší problém vidím v ne vždy bezchybně fungující komunikaci mezi programy, kdy by mohlo docházet k těžko předvídatelným problémům a tím k nefunkčnosti systému, na který je firma velmi vázána. Většina rozšíření, dodávaná externími dodavateli, jsou na takové úrovni, že se stanou přímo součástí systému (dodavatel systému Helios je zakoupí a doplní do systému) a pokud se tomu tak neděje, podnik produkt nezakoupí, protože nechce riskovat narušení stability. Další nevýhodu spatřuji v tom, že vedení i zaměstnanci jsou již na tento systém zvyklí, umí ho dobře a rychle ovládat. U jiného systému (např. s jiným menu) by jim to trvalo zpočátku déle a bylo by nutno projít dalšímu školeními, ke kterým pracovníci nejsou příliš nakloněni.

V teoretické části se zmiňuji, že bezpečnostní politika neobsahuje jména konkrétních lidí. V Edscha Tools jsou na webových stránkách uvedeny přímo konkrétní jména s e-maily a telefony. Navrhoval bych zřídit adresu info@edscha.cz a e-maily přesměrovat na jrathouska@edscha.cz, obdobně zřídit zakaznici@edscha.cz, vedouci-zavodu@edscha.cz, vedouci-vyroby@edscha.cz.

9.1 Modul Přepravní služby

Je modul, který firmě zjednoduší přepravu. Jelikož firma je výrobní podnik, tvoří doprava a přeprava materiálu nebo zboží důležitou část.

Tento modul by firmě zajistil dokonalý přehled o jednotlivých zásilkách ať už na území České republiky nebo i v celé Evropské unii, kam společnost Edscha své výrobky vyváží.

Modul by měl ve spolupráci s CRM (viz další odstavec) centrální adresář odběratelů a dodavatelů, kontaktní osoby, dodací podmínky různých spedičních firem, kódy nákladů a další důležité informace, čímž by došlo k rychlejší evidenci údajů a menší časové náročnosti.

Tento modul umí pracovat ve více měnách, což je praktické pro spediční činnosti v EU, dokáže také podle cenových nabídek jednotlivých firem vykalkulovat cenu, která je pro firmu nejvýhodnější a tím ušetřit finance.

9.2 Modul Styk se zákazníkem

9.2.1 CRM – řízení vztahů se zákazníky

Je další možností rozšíření, ale Edscha Tools není tak velká firma, aby tento modul využívala. O tyto věci se stará ředitel výroby a pracovník odpovědný za obchodní oddělení.

Jeho nasazení by ale mohlo sloužit jako součást havarijního plánu, kdy z nějakých důvodů by oba pracovníci nemohli vykonávat svou činnost pro firmu. Základní problém ale je, že by se všechny kontakty se zákazníky musely do systému zaznamenávat, což je asi největší problém těchto systémů, protože je velmi těžké k tomu uživatele „donutit“.

9.3 Modul Ekonomika

Modul Ekonomika by byl možná pro firmu přínosný, jelikož se týká účetnictví a peněz jako celku, ale firma používá pro tyto věci program SAP, který je nařízen z vedení Edscha AG.

9.4 Modul Manažerské vyhodnocování

Nasazení modulu, který je součástí Helios, by mohlo lépe vystihnout manažerské potřeby svázané s výrobou, než SAP. A mohl by být veden jako další systém k SAP, který by sloužil k porovnání závěrů jednotlivých výstupů.

9.5 Další moduly pro rozšíření

V úvahu by dále mohly přicházet moduly:

- Údržba a servis zařízení,
- Řízení servisních činností,
- Modul Zemědělství by firma, která se zabývá strojírenstvím, nevyužila.

10 IS/IT POUŽÍVANÉ VEDENÍM A TECHNOLOGY

Ve své bakalářské práci chci zmínit specifické technologie, které využívá ředitel výroby a technologové a ke kterým nemají přístup běžní zaměstnanci.

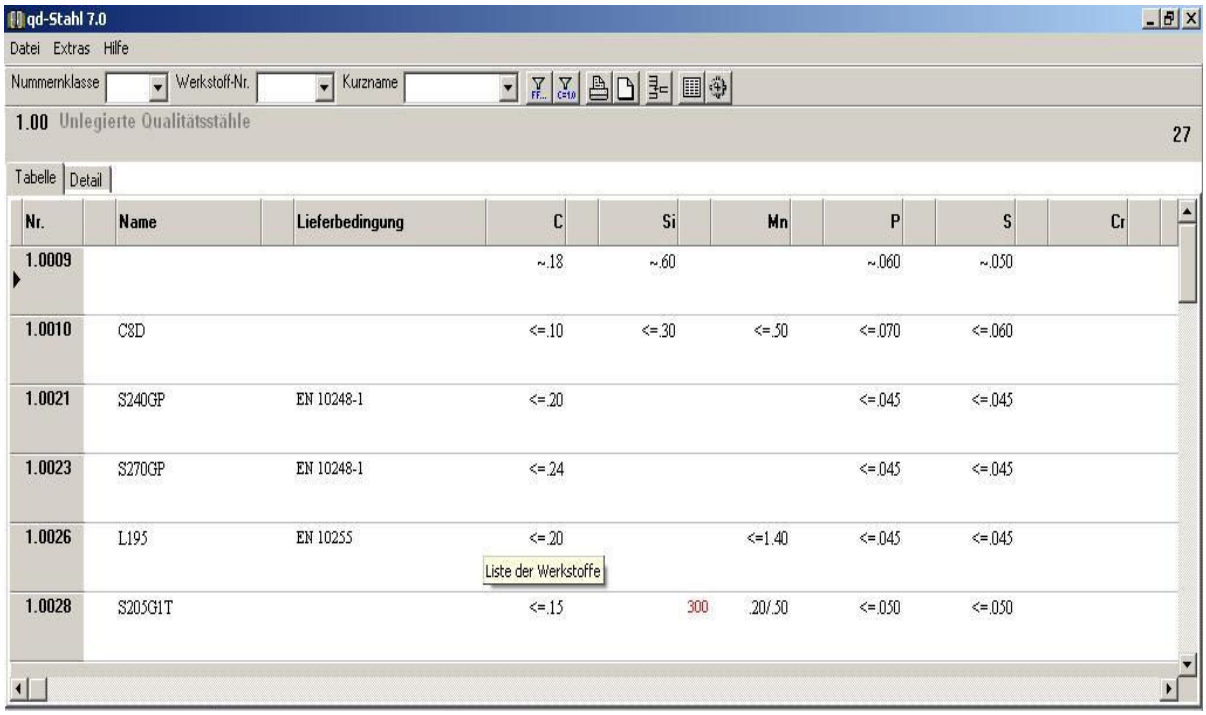
10.1 Hardware a software

Ředitel výroby využívá počítač Compaq Evo D310 s procesorem Intel Pentium 4 2,0 GHz a monitor je LCD Compaq 1701, "17". Toto hardwarové vybavení je plně dostačující. Základní programové vybavení je běžné jako u domácích počítačů, proto se o něm zmíním stručně a zaměřím se jen na programy, které jsou specifické.

Základ tvoří Windows XP Professional (2002), antivirový program AVG, MS Office, internetový prohlížeč Internet Explorer. Pro PDF soubory zde je nainstalovaný Acrobat Reader 5.0, pro videa Quick Time Player a informační systém Helios IQ.

Prvním programem, o kterém bych se rád zmínil, je **COM INFO 1999:** tento program slouží k evidenci zaměstnanců, je napojen na čipové zařízení u vstupu do firmy, kde každý ze zaměstnanců přikládá při příchodu a odchodu svoji čipovou kartu s fotkou na snímač (čipová karta slouží, také k otevření dveří do a z firmy, což přispívá k bezpečnosti). Ředitel výroby má tedy dokonalý přehled o každém pracovníkovi, kolik zaměstnanec odpracoval měsíčně hodin, jaké má přesčasy, kolik zbývá dní dovolené a mnohé další statistiky. Tento program je pouze v Edscha Tools a nemá k němu přístup nikdo jiný než ředitel výroby. Je to samostatný program, který není nijak napojený na systém Helios.

Dalším z programů je **QD – Stahl 6.0 a 7.0,** tyto dva programy jsou specifické pro strojní průmysl, slouží k převádění evropských norem na české. V celé Evropě jsou různé názvy pro materiály a bylo by těžké rozpoznat třeba u zakázky z Francie, z kterého materiálu se má daná zakázka vyrábět.

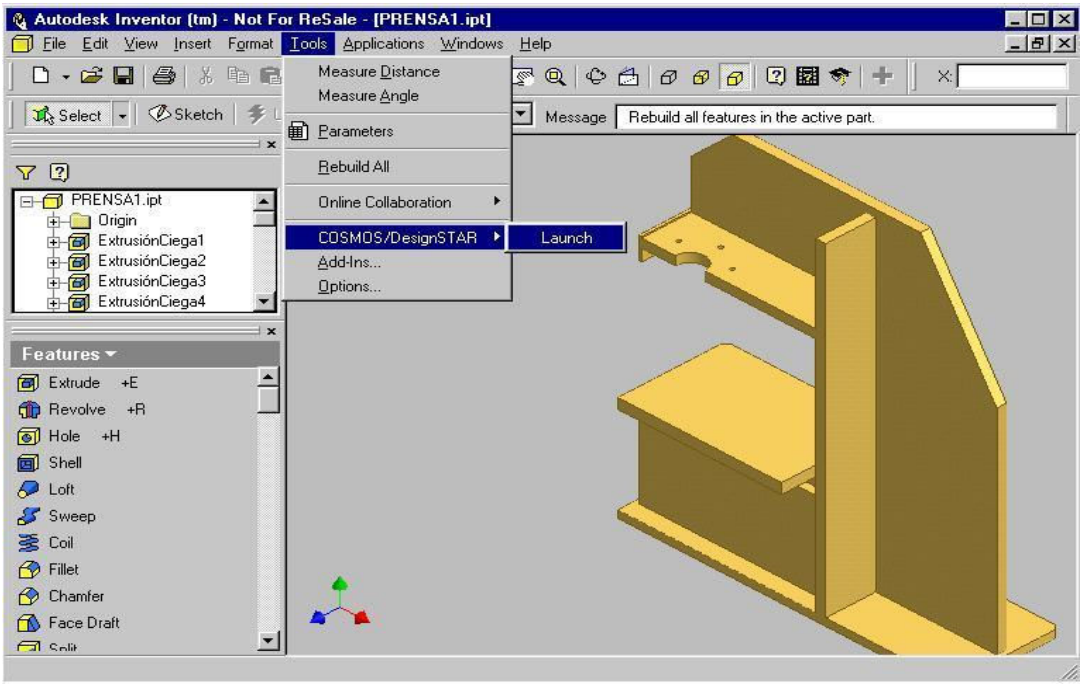


Obrázek 7: Program QD Stahl 7.0

Zdroj: Edscha Tools

Pro technology jako základ slouží Windows XP Professional a další běžné programy jako je MS Office, Akrobat Reader, Avast! Antivirus, Quick Time.

Nejdůležitějším programem, který technologové používají je **Autodesk Inventor 9**. Produkty systému Autodesk Inventor poskytují sadu aplikací pro navrhování a nástroje, které firmě usnadní přechod od 2D ke 3D. Patří sem software Autodesk Inventor Series pro 3D navrhování a dokumentaci, produkty Autodesk Inventor Professional pro vytváření trasovaných systémů a ověřování návrhů, AutoCAD Mechanical pro 2D kreslení a propracování. Systém Autodesk Inventor rovněž obsahuje nový průkopnický přístup k modelování a funkčnímu navrhování.



Obrázek 8: Autodesk Invertor

Zdroj: Edscha Tools

10.2 Mobilní a telefonní komunikace

Služební mobilní telefony, které vedení společnosti Edscha Tools a Edscha Bohemia má, jsou vzájemně „propojeny“, takže se dá mezi nimi volat jen pomocí předčíslí. Stejně funguje i pevná telefonní síť. Není tedy potřeba vytáčet celé telefonní číslo, ale jen již zmíněné předčíslí.

Pevná telefonní linka slouží také k přijímání objednávek, kdy zákazník kontaktuje přímo obchodní oddělení. Vzhledem k tomu, že většina zakázek je z Německa nebo Čech, není problémem komunikace také v němčině. Mluví-li zákazník anglicky, je odkázán na email.

10.3 Internet a síť

Firma Edscha Tools dodržuje podmínky stanovené Edscha AG. Od Edscha AG vedou pevné linky 2-36 Mb, využívající evropských kabelových rozvodů a externích poskytovatelů, které jsou šifrovány, takže se dá velmi snadno poznat, když by chtěl někdo do sítě proniknout zvenčí, ale i zevnitř, pokud k tomu nemá povolení.

V podniku je rozvedena strukturovaná kabeláž. Celý systém kabeláže, pevné telefonní sítě atd. je rozveden z ústředny Triton 3000, která je napojena na hlavní server a ústřednu v Kamenici nad Lipou, odkud je také spravována.

Edscha Tools disponuje připojením rychlostí 2 Mb nejen do internetu, ale i do Virtual Privat Network (VPN) Edscha Gruppe. Pomocí VPN se firma připojuje do Kamenice na Lipou šifrovaným tunelem, který je vytvářen zmíněným proxy serverem (spíše hardwarovým, kvůli větší rychlosti) a teprve tam jdou data do internetu či do jiných provozů dalšími VPN tunely.

Webové stránky má zajištěny pomocí outsourcingu společnosti Czechia[4], další části firmy je mají v současné době v přípravě. Tyto webové stránky jsou podle mne přehledné a srozumitelné a jsou i v dalších světových jazycích, takže zahraniční zákazníci s nimi nemají problémy. Negativum vidím v tom, že jsou velmi statické a možná bych se je snažil doplnit např. o možnost sledování svých zakázek.

[4] http://www.czechia.com

11 BEZPEČNOST A OCHRANA DAT

Firma Edscha Tools klade na bezpečnost a ochranu dat velkou váhu. Je si vědoma toho, že v dnešní době internetu, dochází k napadání počítačů a privátních sítí, a proto se snaží svá data co nejpečlivěji chránit.

Proces komunikace mezi jednotlivými divizemi Edscha AG je zabezpečen v Edscha Tools pomocí proxy serveru.

„Proxy server je server počítačové sítě, který umožňuje klientům nepřímé připojení k jinému serveru. Proxy server funguje jako prostředník mezi klientem a cílovým serverem, překládá klientské požadavky a vůči cílovému serveru vystupuje jako klient. Přijatou odpověď následně odesílá zpět na klienta.“ [16]

Z důvodu bezpečnosti celého systému mi nebyl sdělen typ ani výrobce. Využívá svůj vlastní operační systém a svůj firewall. Slouží k šifrování a dešifrování dat, která jsou odesílána nebo přijímaná z VPN a tím zvyšuje bezpečnost celého systému. Nedochází tedy k používání běžného protokolu. Pomáhá také při zjišťování virů v systému. Systém do dnešního dne nebyl narušen a ani se o to nikdo nepokusil.

Hlavní server není ve firmě Edscha Tools, ale ve firmě Edscha Bohemia. Je to z důvodu finančních nákladů, které jsou se serverem spojeny a z důvodu bezpečnosti. Není nutné zabezpečovat dva servery**,** ale pouze jeden.

Dalším prvkem bezpečnosti je automatická záloha dat, která systém chrání před jejich ztrátou. V tomto podniku není využívána online replikace dat. Záloha dat se provádí výhradně v noci a došlo-li by k nabourání systému a vymazání dat, nebo k nějakým technickým problémům systému, chybělo by maximálně posledních 24 hodin.

Data jsou ukládána mimo firmu. Je využíváno outsourcingové společnosti, která spolupracuje s celou Edscha AG. Datový sklad pro celou společnost je ve Frankfurtu nad Mohanem.

Před výpadkem proudu jsou důležité počítače chráněny pomocí záložních zdrojů UPS (Uninterruptible Power Supply (Source) – „nepřerušitelný zdroj energie“), které dodávají energii při výpadku elektrické sítě pro ukončení práce počítačů, filtrují poruchy, které se objevují v napájecí síti, jako jsou napěťové špičky. Energie je čerpána při výpadku napájecí sítě z vestavěných baterií.

Pro bezpečnost před viry je v počítačích využíván v celém podniku systém AVG.

Při přístupu do sítě se musejí všichni uživatelé zalogovat svým uživatelským jménem a heslem. Podle toho systém pozná, který uživatel se připojil a jaká oprávnění tento uživatel má.

Je rozdíl přihlásí-li se technolog, nebo přihlásí-li se ředitel výroby. Každý uživatel má pouze určitá oprávnění k programům a aplikacím, které pro svoji práci potřebuje. Technolog např. nepotřebuje mít přístup k docházce zaměstnanců na rozdíl od ředitele výroby, který rozhoduje o odměnách nebo o udělení dovolené.

Tyto oprávnění může měnit podle potřeby pouze Ing. Kupka, který k takovým věcem má jedinečný přístup. Ing. Kupka také může kontrolovat, kdo je zrovna nalogován, se kterými operacemi uživatel pracuje, jak dlouho se odmlčel a zpětně se dají dohledat kroky, které jakýkoliv zaměstnanec v dřívější době učinil. Nemá však přístup např. k docházkovému programu COM INFO nebo ke mzdám. Tento přístup se mi nezdá úplně bezpečný a správný a vidím v tom určité riziko, které by se snížilo tím, že by neměl veškerá oprávnění a např. druhá osoba by mohla dohledat jeho kroky, které učinil a ten by je musel vysvětlit.

12 IS PRO ZAMĚSTNANCE

IS Edscha Tools využívají pouze někteří zaměstnanci. Běžní dělníci počítače a jejich technologie ke své práci nepotřebují. Využívají pouze jejich produktů, jako jsou výkresy a programy pro CNC centra.

Osoby pracující ve skladu, mají přistup pouze k aplikacím, starající se o skladové položky a jejich objednávání. Objednávky musí schvalovat ředitel výroby. Jejich přihlášení probíhá opět pomocí přístupového jména a hesla. Jejich oprávnění jsou tedy velmi omezená.

Pracovníci a pracovnice pracující v kancelářích mají opět přístup k programům, které při práci používají, jako jsou účetní a daňové programy, internet apod.

Podle mého názoru je to zde správně řešeno a není důvodu, aby všichni zaměstnanci měli přístup ke všemu.

12.1 Možnosti rozšíření

12.1.1 Internet pro zaměstnance

Rozšíření IS bych viděl v možnosti přístupu zaměstnanců na internet, kde by pro ně mohla být vyčleněna místnost s počítačem, který by mohli po pracovní době využívat. A bylo by dobré, kdyby to byl počítač jen pro internet, aby nedošlo k zneužití dat majitele PC.

12.1.2 Zaměstnanecký portál-elektronické nástěnky

Zaměstnanci si mohou číst informace od vedení i jinde než ve firmě, pochopitelně přes zabezpečený přenos. Obsahem by mohly být vnitřní směrnice, plány dovolených, aj.

12.1.3 Předávání podnětů, zlepšovacích návrhů

Zaměstnance může vedení také kontaktovat podle určitých pravidel, jedna možnost by byla i anonymně.

12.1.4 Odborová agenda

Pokud v organizaci působí odbory a mají dobrý vztah k vedení, je možné jim umožnit v rámci podnikového intranetu různé služby, typicky vybírání příspěvků.

ZÁVĚR

Cílem mé práce bylo popsat IS/IT ve firmě Edscha Tools a.s., bezpečnost tohoto systému, zaměřit se na využití IS při plánování výroby a komunikaci se zákazníkem a popsat IS/IT vedení firmy a zaměstnanců. Myslím si, že jsem tomuto úkolu věnoval dostatečné úsilí a výsledkem je podrobné popsání těchto věcí a navrhnutí některých inovací.

PIS dnes neodmyslitelně patří k fungujícímu a prosperujícímu podniku, bez nich by nebylo možno uspět na konkurenčním trhu. Zjednodušují práci nejenom podniku., ale i zákazníkům a přispívají tak k rychlejšímu vyřízení zakázek a s nimi spojených formalit.

Po nastudování teoretické části z odborné literatury a návštěvy pana Ing. Kupky, který je za IS/IT zodpovědný, mi bylo řečeno, že ne vždy se všechno řídí teoretickými poučkami a „chytrými větami“, ale jde především o hledání kompromisů a optimálních řešení, protože každý systém v každé jednotlivé organizaci je do jisté míry jedinečný a individuální. Co funguje v organizaci jedné, nemusí stejně dobře fungovat v organizaci druhé a to jak po stránce hardwaro-softwarové, tak i lidské.

Systém Helios hodnotím velmi pozitivně a po schůzkách s jednotlivými lidmi jsem nezaznamenal žádné negativní reakce. Pracovníci jsou na něj zvyklí a jsou s ním spokojeni. Ani já jsem nezaznamenal žádná negativa. Mohl by se jen rozšířit o moduly, o kterých se v práci zmiňuji.

Zabezpečení shledávám jako plně dostačující, ale o jeho kvalitě se firma může přesvědčit až při útoku. Probíhají sice simulované testy napadení, kdy systém pracuje spolehlivě, ale realita může být jiná.

Negativa shledávám v určitých nařízeních od Edscha AG. Nemožnosti přímé komunikace v angličtině, ale pouze pomocí e-mailu nebo externího tlumočníka. Myslím si, že nejvyšší oprávnění by měla být rozdělena mezi dva pracovníky.

Do budoucna firma plánuje pořízení vlastního serveru do Edscha Tools a.s. a výměnu některých starých počítačových jednotek za novější a výkonnější.

Tato práce mne velmi obohatila a domnívám se, že jsem systém velmi dobře pochopil a nedokážu si představit, že by firma mohla bez něj fungovat.

LITERATURA

[1] Sodomka, P.: Informační systémy v podnikové praxi. Brno: Computer Press, 2006, str. 44

[2] Kolektiv autorů: Časopis IT Systems. Praha: CCB, spol s r. o., 4/2005, str. 28 - 44

[3] Hanáček, P., Staudek, J.: Bezpečnost informačních systémů, ÚSIS, Praha, 2000

[4] Gála, P., Pour, J., Toman, P.:Podniková informatika, Praha: Grada Publishing, a.s., 2006

Webové odkazy

cit: červenec 2007

[5] http://www.helios.eu/

[6] http://www.systemonline.cz

[7] http://www.edscha.cz

[8] http://www.cvis.cz/hlavni.php?stranka=novinky/clanek.php&id=292&PHPSESSID=19f5eac7106c6724ac36d7bd3244df4c

[9] http://nb.vse.cz/~vorisek/FILES/Clanky/1996_Csf_a_rizika_IS.htm

[10] http://www.deltax.cz/dtx2004/default.aspx?j=33&obl=1&k=2541&o=23&d=15632

[11] http://casopis.systemonline.cz/292-uskali-zavadeni-is-it-ve-firme.htm

[12] http://www.systemonline.cz/outsourcing-ict/outsourcing-it-v-praxi.htm

[13] http://www.systemonline.cz/clanky/neduvera-k-outsourcingu-je-draha.htm

[14] http://www.systemonline.cz/clanky/outsourcing-it.htm

[15] http://www.helios.eu/?lg=cs&cm=orange&pg=info

[16] http://cs.wikipedia.org/wiki/Proxy_server

SEZNAM OBRÁZKŮ

SEZNAM TABULEK