

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH
PEDAGOGICKÁ FAKULTA

katedra fyziky

Studijní obor: Měřicí a výpočetní technika

BAKALÁŘSKÁ PRÁCE

**Využití internetu jako zdroje informací pro zákazníky energetických
společností**

Knihovna JU - PF



Vedoucí práce:

RNDr. František Špulák

Autor:

Martin Špika

2005

Prohláším, že jsem během své práce na této práci vyhledal všechny relevantní informace pro získání co nejúplnějšího přehledu o dané problematice, práci s použitím vhodné literatury.

Touto cestou si dovoluji poděkovat vedoucímu diplomové práce RNDr. Františku Špulákovi za jeho odbornou pomoc a ochotu při vypracování této práce.

1. ÚVOD	1
2. CÍLE A PŘEDMĚT PRÁCE	2
3. METODIKA PRÁCE	3
4. VÝVOJ ENERGETICKÝCH SPOLEČNOSTÍ	4
4.1. Úvodní kapitola	4
4.2. Historie energetických společností	5
4.3. Současný stav energetických společností	6
4.4. Budoucnost energetických společností	7
5. VYUŽITÍ INTERNETU JAKO ZDROJE INFORMACÍ	8
5.1. Úvodní kapitola	8
5.2. Historie internetu	9
5.3. Současný stav internetu	10
5.4. Budoucnost internetu	11
6. VYUŽITÍ INTERNETU ENERGETICKÝMI SPOLEČNOSTMI	12
6.1. Úvodní kapitola	12
6.2. Historie využívání internetu energetickými společnostmi	13
6.3. Současný stav využívání internetu energetickými společnostmi	14
6.4. Budoucnost využívání internetu energetickými společnostmi	15
7. ZÁVĚR	16
8. PŘÍLOHY	17
8.1. Příloha A	17
8.2. Příloha B	18
8.3. Příloha C	19
8.4. Příloha D	20
8.5. Příloha E	21
8.6. Příloha F	22
8.7. Příloha G	23
8.8. Příloha H	24
8.9. Příloha I	25
8.10. Příloha J	26
8.11. Příloha K	27
8.12. Příloha L	28
8.13. Příloha M	29
8.14. Příloha N	30
8.15. Příloha O	31
8.16. Příloha P	32
8.17. Příloha Q	33
8.18. Příloha R	34
8.19. Příloha S	35
8.20. Příloha T	36
8.21. Příloha U	37
8.22. Příloha V	38
8.23. Příloha W	39
8.24. Příloha X	40
8.25. Příloha Y	41
8.26. Příloha Z	42
8.27. Příloha AA	43
8.28. Příloha AB	44
8.29. Příloha AC	45
8.30. Příloha AD	46
8.31. Příloha AE	47
8.32. Příloha AF	48
8.33. Příloha AG	49
8.34. Příloha AH	50
8.35. Příloha AI	51
8.36. Příloha AJ	52
8.37. Příloha AK	53
8.38. Příloha AL	54
8.39. Příloha AM	55
8.40. Příloha AN	56
8.41. Příloha AO	57
8.42. Příloha AP	58
8.43. Příloha AQ	59
8.44. Příloha AR	60
8.45. Příloha AS	61
8.46. Příloha AT	62
8.47. Příloha AU	63
8.48. Příloha AV	64
8.49. Příloha AW	65
8.50. Příloha AX	66
8.51. Příloha AY	67
8.52. Příloha AZ	68
8.53. Příloha BA	69
8.54. Příloha BB	70
8.55. Příloha BC	71
8.56. Příloha BD	72
8.57. Příloha BE	73
8.58. Příloha BF	74
8.59. Příloha BG	75
8.60. Příloha BH	76
8.61. Příloha BI	77
8.62. Příloha BJ	78
8.63. Příloha BK	79
8.64. Příloha BL	80
8.65. Příloha BM	81
8.66. Příloha BN	82
8.67. Příloha BO	83
8.68. Příloha BP	84
8.69. Příloha BQ	85
8.70. Příloha BR	86
8.71. Příloha BS	87
8.72. Příloha BT	88
8.73. Příloha BU	89
8.74. Příloha BV	90
8.75. Příloha BW	91
8.76. Příloha BX	92
8.77. Příloha BY	93
8.78. Příloha BZ	94
8.79. Příloha CA	95
8.80. Příloha CB	96
8.81. Příloha CC	97
8.82. Příloha CD	98
8.83. Příloha CE	99
8.84. Příloha CF	100

Prohlašuji, že jsem bakalářskou práci na téma „Využití internetu jako zdroje informací pro zákazníky energetických společností“ vypracoval samostatně, pouze s použitím citované literatury.

V Českých Budějovicích 30.11. 2005.



1	ÚVOD	4
2	BEZPEČNOST INFORMAČNÍCH SYSTÉMŮ	6
2.1	MOTIVACE PRO ZABEZPEČOVÁNÍ PŘI POUŽITÍ IT	6
2.2	ZAJIŠTĚNÍ BEZPEČNOSTI INFORMAČNÍHO SYSTÉMU	10
2.2.1	<i>Jak přistoupit k zajištění bezpečnosti IS</i>	10
2.2.2	<i>Povědomí všech zaměstnanců o bezpečnosti IS</i>	11
2.2.3	<i>Výběr a implementace vhodných technických opatření</i>	12
2.3	BEZPEČNOSTNÍ STUDIE	12
2.3.1	<i>Přínosy zpracování bezpečnostní politiky</i>	12
2.3.2	<i>Rozsah bezpečnostní studie</i>	13
2.3.3	<i>Cíle informační bezpečnosti</i>	13
2.3.4	<i>Definování aktiv</i>	14
2.3.5	<i>Odhad hrozeb</i>	14
2.3.6	<i>Analýza zranitelností</i>	14
2.3.7	<i>Odhad dopadů</i>	15
2.3.8	<i>Analýza rizik</i>	15
2.3.9	<i>Přijetí zbytkových rizik</i>	15
2.3.10	<i>Stanovení omezení</i>	16
2.4	RIZIKA	16
2.4.1	<i>Prolomení hesla hrubou silou</i>	16
2.4.2	<i>Prolomení hesla sociálním útokem</i>	17
2.4.3	<i>Hardwarové útoky</i>	18
3	INTEGRACE PODNIKOVÝCH APLIKACÍ	20
3.1	PROČ POTŘEBUJEME INTEGROVAT PODNIKOVÉ APLIKACE	20
3.2	NADBYTEČNÉ NÁKLADY	20
3.3	NEVHODNÁ ŘEŠENÍ	20
3.4	PRUŽNĚ PROTI KONKURENCI	21
3.5	NÁSTUP EAI	21
3.6	EKONOMICKÝ POHLED	21
3.7	Z POHLEDU PROCESNÍHO ŘÍZENÍ	22
3.8	CO ROZHODUJE V IT ODDĚLENÍ	22
4	JAK FUNGUJÍ A CO NABÍZEJÍ MODERNÍ INTEGRAČNÍ PLATFORMY	24
4.1	OTÁZKY PRO MANAŽERY	24
4.2	KUDY NELZE JÍT	25
4.3	JAK FUNGUJE EAI ŘEŠENÍ	25
4.4	PROPOJENÍ PŘES DATA	25
4.5	UŽIVATELSKÉ ROZHRANÍ A PORTÁL	26
4.6	PŘÍLIŠ TĚSNÉ PROPOJENÍ	27
4.7	ORIENTACE NA SLUŽBY - SOA	27

4.8	CO NABÍZÍ MODERNÍ EAI	28
4.9	SPECIALIZOVANÉ PLATFORMY.....	28
4.10	NABÍDKA PRO VŠECHNY	28
5	PORTÁLY	30
5.1	ARCHITEKTURA PORTÁLU	30
5.2	KLÍČOVÉ RYSY PORTÁLU.....	31
5.3	BEZPEČNOST	31
5.4	PORTÁL JAKO INTRANET.....	32
5.5	EXPANZE ZA HRANICE	32
5.6	MOBILNÍ PŘÍSTUP	32
5.7	PŘÍNOSY A RIZIKA	33
6	VLIV PORTÁLOVÝCH ŘEŠENÍ NA PROVOZ PODNIKOVÝCH INFORMAČNÍCH SYSTÉMŮ	34
6.1	OD HISTORIE K AKTUÁLNÍ NABÍDCE	34
6.2	URČENÍ KRITÉRIA ÚSPĚCHU.....	35
6.3	POMOC S INTEGRACÍ.....	35
6.4	PROPOJENÍ S PARTNERY.....	35
6.5	WEBOVÉ SLUŽBY.....	36
7	VYUŽITÍ CRM V ENERGETICKÉ FIRMĚ	37
7.1	VŠEOBECNÉ SOUVISLOSTI	37
7.2	KDO IMPLEMENTUJE CO.....	37
8	PROBLEMATIKA PRAKTICKÉHO VYUŽITÍ DVOU TYPŮ PORTÁLŮ	42
8.1	SLUŽBY VELKOODBĚRATELŮM NA INTERNETU (JČE).....	42
8.1.1	<i>Technický popis</i>	42
8.1.2	<i>Přehled funkcí</i>	43
8.1.2.1	Přihlášení.....	43
8.1.2.2	Homepage portálu	43
8.1.2.3	Statistika odběru.....	44
8.1.2.4	Detailní statistika odběru.....	46
8.1.2.5	Grafické zobrazení	47
8.1.2.6	Stanovení optimální sazby.....	47
8.1.2.7	Zasílání faktury	49
8.1.2.8	Help.....	50
8.2	PORTÁL PRO VELKOODBĚRATELE (E.ON)	51
8.2.1	<i>Technický popis</i>	52
8.2.2	<i>Technologické řešení</i>	54
8.2.3	<i>Infrastruktura</i>	55
9	ZÁVĚR.....	57
9.1	WEBOVÉ SLUŽBY.....	57

9.2	POROVNÁNÍ PORTÁLŮ	58
10	LITERATURA	60
10.1	INTERNETOVÉ ZDROJE	61

1 Úvod

Odezvy portálových řešení a technologií již dnes mají značný dopad na provoz podnikových informačních systémů. Prakticky všechny větší firmy projevují zájem o možnosti portálového řešení. Uživatelé se jednoznačně odklánějí od tradičních klientských aplikací ERP systému a žádají „tenkého“ klienta bez potřeby jakékoliv instalace na straně koncového PC s integrovaným přístupem ke všem aplikacím (ať už SAP, Microsoft, atd...) v prostředí internetového prohlížeče – přístup pomocí portálu.

Z provozního hlediska je vidět značná úspora pracnosti pro pracovníky IT v oblasti správy koncových PC, jednodušší administraci celého systému včetně správy oprávnění, centrální správy uživatelů a možnosti integrovaného přístupu k bezpečnostní politice společnosti. Součástí interního portálu obvykle bývá funkčnost Knowledge Managementu, jenž obsahuje mimo jiné nástroje pro podporu oběhu elektronických dokumentů ve firmě (webflow) a správu dokumentů v celém jejich životním cyklu (DMS - document management system) včetně jejich klasifikace, vyhledávání a společného sdílení virtuálními týmy či diskusí nad nimi v elektronických diskusních a projektových místnostech.

V internetových portálech se stále ve větší míře začíná využívat technologie zvaná Web Services. Web Services nejsou v České republice zatím tak rozšířeny jako v jiných vyspělých zemích. Nedostatek finančních prostředků v komerční sféře a nekonceptnost státní správy v oblasti systémové integrace nedávají v současné době velké předpoklady pro jejich rychlé rozšíření do praxe. Samozřejmě že zvýšený zájem o tyto služby je u českých firem patrný, hlavně u větších společností, ale ten pravý "boom" nás teprve čeká.

Důležitým faktorem je akutní potřeba výměny dat. Český zákazník si pro ni musí vytvořit nebo mít vytvořeny ekonomické, technické, technologické i legislativní podmínky. Ruku v ruce s tím jde i vývoj odpovídajících cenově dostupných produktů a informovanost od firem, které se tímto vývojem zabývají. Přitom nelze nezmínit výhody i rizika, které nasazení Web Services přináší.

Možný scénář zavedení do praxe může být zcela prozaický. V zájmu udržení konkurenceshopnosti budou firmy donuceny zpřístupnit data a nabízet své služby pomocí webového rozhraní - portálu. V této rovině mají Web Services velký potenciál a bude tedy především na vývojářských firmách, jestli dokáží v pravý čas nabídnout ten správný produkt.

Bakalářská práce shrnuje problematiku rozsáhlých informačních systémů velké firmy a jejich spojitost se vztahem k zákazníkovi. Především se zaměřím na přístup k zákazníkům pomocí internetu a zákaznického portálu, kde v současné době hraje technologie zvaná web services stále důležitější roli. Dále jsou zmíněny otázky bezpečnosti a rizika napadení informačních systémů, včetně zásad vypracování bezpečnostní studie. Jsou zde objasněny principy moderních integračních platform a jejich využití při integraci podnikových aplikací. Porovnání dvou portálových řešení energetické firmy ukazuje konkrétní přístup k tomuto problému. Zároveň můžeme posoudit vývoj IT technologií, protože první z popisovaných řešení bylo nasazeno již v roce 2001 a druhé bude zprovozněno na začátku roku 2006.

2 Bezpečnost informačních systémů

Informační technologie zpracovávají stále více a více informací s velkou hodnotou. Pokud hovoříme v souvislosti s informačními technologiemi o zpracovávání informací, pak tím rozumíme použití těchto technologií k uchovávání, přenosu, vyhodnocování a prezentaci informací. Poněvadž se mnohdy jedná o informace s nezanedbatelnou hodnotou (např. zdravotní záznamy, daňová přiznání, bankovní účty, elektronické platební nástroje, výsledky vývoje nebo výzkumu, obchodní záměry), musí být chráněny tak:

- aby k nim měly přístup pouze oprávněné osoby
- aby se zpracovávaly nefalšované informace
- aby se dalo zjistit, kdo je vytvořil, změnil nebo odstranil
- aby nebyly nekontrolovaným způsobem vyzrazeny
- aby byly dostupné tehdy, když jsou potřebné.

2.1 Motivace pro zabezpečování při použití IT

Narušení bezpečnosti zpracovávání informací lze provést například:

- narušením soukromí či utajení informací
- vydáváním se za jinou oprávněnou osobu a zneužíváním jejích privilegií
- distancováním se od odpovědnosti nebo od závazků plynoucích z manipulace s informacemi
- tvrzením, že se nějaká informace někam poslala a toto se nikdy nestalo
- tvrzením, že se informace získala od nějakého podvodníka
- neoprávněným zvýšením svých privilegií přístupu k informacím
- modifikací privilegií ostatních osob
- zatajením výskytu důvěrné informace v jiných informacích
- zjišťováním, kdo a kdy si zpřístupňuje které informace
- zařazením se jako skrytý mezičlánek v konverzaci jiných subjektů
- pokažením funkcionality softwaru doplněním skrytých funkcí
- narušením protokolu činností jiných subjektů zavedením nesprávných, nekorektních informací
- podkopáním důvěryhodnosti protokolu způsobeným zjevným, byť možná jen zdánlivými poruchami
- bráněním jiným uživatelům legitimně komunikovat.

Charakteristickým rysem soudobých organizací tedy je, že svoje poslání plní pomocí propojení informačních a komunikačních systémů budovaných na bázi IT, a to jak uvnitř organizace (intra..., lze připomenout pojem „intranet“, vnitřní síť), tak i s ostatními organizacemi (extra... / inter..., např. „extranet“ / Internet). Tím se činnosti organizace stávají silně závislé na informacích a službách IT. Důsledkem je, že ztráta důvěrnosti, integrity, dostupnosti, prokazatelnosti odpovědnosti, autenticity a spolehlivosti informací a služeb IT má na chod organizace nepříznivý dopad. Řešením je uplatnění zásad bezpečnosti IT. Pojmem zabezpečování IT označujeme proces dosažení a udržení důvěrnosti, integrity, dostupnosti, prokazatelnosti odpovědnosti, autenticity a spolehlivosti informací a služeb IT na přiměřené úrovni [8].

Vhodným metodickým průvodcem bezpečností IT je např. technická zpráva ISO/IEC TR 13335 „Information technology – Guidelines for the Management of IT Technology“. Podle tohoto materiálu se bezpečnost IT použitých v organizaci dosahuje především plněním manažerských funkcí, souvisejících s bezpečností IT jako integrální součástí plnění globálního plánu správy organizace. Mezi takové manažerské funkce typicky patří:

- určení cílů, strategií a politik zabezpečení IT organizace
- určení požadavků na zabezpečení IT organizace
- identifikace a analýza hrozeb pro aktiva IT v rámci organizace
- identifikace a analýza rizik pro organizaci plynoucích z používání IT
- specifikace přiměřených bezpečnostních opatření eliminujících nebo snižujících rizika
- sledování implementace a provozu bezpečnostních opatření použitých pro účinnou ochranu informací a služeb IT v rámci organizace
- vyvinutí a zavedení programu zvyšování bezpečnostních znalostí a vědomí nutnosti udržovat bezpečí všech, kdo IT v organizaci používají
- detekování bezpečnostních incidentů a adekvátní reakce na ně.

Organizace musí své informační systémy zabezpečovat stejně jako jiné investice do své činnosti. Hardwarové komponenty IT lze zničit (teroristy nebo i nespokojenými či pomatenými zaměstnanci) nebo ukrást (a levně prodat nebo používat pro vlastní potřebu). „Ukrást“ lze i software, který mnohdy představuje enormní a přitom špatně vyčíslitelné hodnoty. Konkurent tak může ušetřit náklady na vývoj a/nebo na pořízení softwaru. Neoprávněné užívání softwaru zaměstnanci pro osobní potřebu nebo pro jejich druhé zaměstnání je zdrojem jejich nelegálních zisků. Provozovateli kradeného

softwaru mohou vzniknout škody plynoucí z trestní odpovědnosti za porušení licence. Informační systém lze používat neautorizovaně, a tím způsobit např. zničení systému nebo porušení soukromí jiných osob („krádeží“ přístupového hesla, překonáním mechanismu řídicího přístup k IS) nebo lze využívat IS i autorizovanými zaměstnanci k nepracovní činnosti, ať již osobní, nebo výdělečné.

Informace jsou v podstatě zboží, pro organizaci představují mnohdy cenná aktiva. Data uložená v bázích dat lze ukrást neoprávněným okopírováním, lze ukrást i výstupy generované IS pro potřebu organizace. Data, která jsou pro organizaci citlivá, je potřeba chránit před konkurencí. Existují právní, morální a etická pravidla pro používání informací, existují zákonné úpravy pro ochranu dat, a ty je žádoucí, resp. nutné, dodržovat.

Organizace se musí bránit tomu, aby funkce jejich IS nebyly ať již zlomyslně, nebo neúmyslně znepřístupněny.

IT specialista musí z titulu své funkce nebo pracovní náplně řešit především problémy související:

- s vývojem bezpečnostní politiky IT
 - s identifikací rolí a odpovědností za data a IT v organizaci
 - se správou rizik organizace
 - identifikace, zvládnutí, odstranění nebo minimalizace událostí, které mají nežádoucí vliv na činnost a aktiva organizace
 - identifikace a ohodnocení chráněných aktiv, citlivých dat a jejich klasifikace do tříd vymezujících potřebnost jejich ochrany
 - identifikace zranitelných míst v používaných IT a s nimi souvisejících hrozeb
 - určení forem útoků a typu útočníků
 - určení pravděpodobností útoků, tj. jakým rizikům jsou IS organizace vystaveny, včetně určení potenciálních škod
 - respektovaných omezení organizačních, finančních, daných prostředím, personálních, časových, právních, technických, kulturně–sociálních apod.).
- Získané znalosti zákazníkovi usnadní porozumět problémům, které souvisejí
- s principy, postupy
 - s výběrem bezpečnostních opatření a s jejich implementací vhodnými bezpečnostními mechanismy
 - se správou konfigurace IS
 - se správou změnového řízení v použitých IT

- s vypracováním havarijních plánů určujících činnost organizace po narušení bezpečnosti
- s vlastní bezpečnou provozní činností v oblasti IT organizace (zajišťování údržby IS, bezpečnostní auditorské činnosti, monitorování, vyhodnocování činností IS, reakce na bezpečnostní incidenty).

V neposlední řadě se lidé, kteří se starají o bezpečnost IT, musí zabývat i školicími aktivitami v oblasti bezpečnosti.

Dále je nutné upozornit, že bezpečnost IT nelze řešit izolovaně. Bezpečnostní politika v oblasti IT je nedílnou součástí všeobecné bezpečnostní politiky organizace, která představuje souhrn bezpečnostních zásad a předpisů definujících způsob zabezpečení organizace od fyzické ostrahy, přes ochranu profesních zájmů až po ochranu soukromí a lidských práv.

Bezpečnostní politika IT organizace (také celková bezpečnostní politika IT) se v tomto kontextu zabývá výběrem bezpečnostních zásad a předpisů splňujících bezpečnostní politiku organizace a obecně definujících bezpečné používání informačních zdrojů v rámci organizace nezávisle na konkrétně použitých informačních technologiích (určuje, která data jsou pro organizaci citlivá, kdo je za ně odpovědný, předpisuje infrastrukturu zabývající se v rámci organizační struktury organizace bezpečností, vymezuje základní omezení, která se musí respektovat apod.).

Určení detailních konkrétních norem, pravidel, praktik, předpisů konkrétně definujících způsob správy, ochrany, distribuce citlivých informací a jiných konkrétních informačních zdrojů v rámci organizace, specifikace bezpečnostních opatření a způsobu jejich implementace, určení způsobu jejich použití, který zaručuje přiměřenou bezpečnost odpovídající požadavkům bezpečnostní politiky IT organizace, při respektování konkrétně použitých IT pro realizaci IS organizace, to vše je náplní bezpečnostní politiky IS organizace (také systémové bezpečnostní politiky IT).

Provozní prosazování systémové bezpečnostní politiky se často označuje pojmem bezpečnostní program.

Ani všeobecnou bezpečnostní politiku organizace nelze řešit bez návaznosti na ostatní politiky vymezující chod a poslání organizace (finanční, obchodní, sociální atd.).

Důležité je si uvědomit, že zkušenosti útočníků v čase rostou, cíle jejich útoků se postupně upřesňují, informační technologie se vyvíjejí a zdokonalují, mění se případně i cíle profilu organizace. Proto se i cíle, strategie a politiky bezpečnosti musí periodicky korigovat. Vhodné jsou periodické oponentury bezpečnostních politik, které mohou

vyvolat požadavek opakovaného provedení analýzy rizik, periodicky je potřebné provádět i bezpečnostní audit [8].

2.2 Zajištění bezpečnosti informačního systému

Zajištění bezpečnosti spravovaného informačního systému je problém, který není u žádného správce příliš oblíbený. Toto není způsobeno pouze složitostí a rozsáhlostí problematiky, ale z velké části také otázkami lidského faktoru.

2.2.1 Jak přistoupit k zajištění bezpečnosti IS

V první řadě je třeba si vytvořit přehled oblastí, které jsou potenciálně rizikové. Následně je třeba zvážit co a do jaké míry je těmito riziky ohroženo a na tomto základě stanovit okrajové podmínky a pravidla pro zajištění bezpečnosti informačního systému.

Zde doporučuji následující systém řízení bezpečnosti:

- vývoj politiky bezpečnosti informačních technologií
- identifikaci rolí a odpovědností uvnitř organizace
- řízení konfigurace informačních systémů
- řízení změn
- povědomí všech zaměstnanců o bezpečnosti informačních systémů
- výběr a implementace vhodných ochranných opatření
- havarijní plány a plánování obnovy systémů a dat po havárii
- management rizik, včetně identifikace a odhadu:
 - aktiv, která je třeba chránit
 - hrozeb
 - zranitelností
 - dopadů
 - rizik
 - ochranných opatření
 - zbytkových rizik
 - omezení
- následující včetně:
 - údržby
 - bezpečnostního auditu
 - monitorování
 - revize
 - zacházení s incidenty

Po zpracování této problematiky je možno přistoupit ke zpracování cílů, strategie a bezpečnostní politiky informačního systému.

Velmi důležitým faktorem při rozboru a řešení problematiky bezpečnosti je komplexní pohled. Ne vždy jsou použita řešení vyvážená, celistvá a stává se, že neodpovídají skutečným potřebám a požadavkům. Nevyváženost může být způsobena zaměřením se na oblast technického zabezpečení, která je v momentální situaci nejvíce v "kurzu" a opomíjením dalo by se říci "lidského" zabezpečení. Málokdo si uvědomuje, že jde o neméně důležitou součást, která spolu s technickými prostředky tvoří nedílný celek zabezpečení informačního systému. Jinak řečeno, jestliže při zabezpečování našeho systému volíme vyspělou techniku a důmyslný systém opatření proti útokům zvenčí, měli bychom současně s tím i důkladně vyřešit problematiku týkající se útoků zevnitř. To co zaručí anebo nadobro zničí úspěch ochrany není jen samotné technické řešení, ale také uplatňování organizačních pravidel. Ta by měla být řešena i v rámci životního cyklu informačního systému.

Celý systém řízení bezpečnosti tak můžeme rozdělit na dvě části:

2.2.2 Povědomí všech zaměstnanců o bezpečnosti IS

Pro správnou funkci bezpečnostních opatření je zapotřebí dodržovat základní pravidla při práci s počítačovými systémy. To znamená, že si uživatelé navzájem nesdělují přístupová jména, hesla a přístupové kódy. Samozřejmě je nikomu nedávají napsaná, s výjimkou zapečetěných obálek v trezoru, které se otevírají při mimořádných krizových situacích. Samozřejmostí je, že uživatelé si svá hesla a přihlašovací jména nezapisují na volně přístupná místa. Typickým zlovykem jsou lístečky nalepené na monitorech či klávesnicích. Také při volbě hesla či kódu je vhodné zvolit takový systém, aby heslo nebo kód nebyl lehce odvoditelný. Vysloveně nevhodné je vlastní jméno či příjmení, jména dětí, manžela či manželky, datumy narození, svátků a rodná čísla. Obzvláštní obezřetnost je na místě, pracuje-li se prostřednictvím internetu. Kromě již uvedeného je nutné pečlivě dodržovat nařízení týkající se zasílání a přijímání nepovolených typů příloh, stahování jakýchkoliv neznámých aplikací nebo samospustitelných souborů, navštěvování nepovolených či rizikových www stránek a podobně. Správné nastavení firewallu či pravidel proxyserveru může nežádoucí rizikové chování uživatelů výrazně omezit, nicméně nevyloučí jej nikdy. Proto je potřeba, aby sami uživatelé dodržovali základní pravidla bezpečnosti.

Druhou součástí systému řízení bezpečnosti je:

2.2.3 Výběr a implementace vhodných technických opatření

Tím můžeme rozumět např. zavedení přístupových karet, omezení práv přístupu uživatelů k datům podle jejich skutečných potřeb a stupně důležitosti dat, nastavení práv uživatelů komunikujících prostřednictvím internetu, protivirovou kontrolu veškeré komunikace směřující dovnitř i ven z vnitřní sítě a podobně. Zajištění technické části bezpečnosti lze dosáhnout pomocí správného nastavení firewallů, volbou vhodné vnitřní architektury sítě a mnoha dalšími způsoby.

Při posuzování bezpečnosti je třeba si uvědomit, že každý systém je silný jen tak, jak silný je jeho nejslabší článek. V případě zabezpečení informačních systémů je nejslabším článkem jednoznačně uživatel.

Jako příklad lze uvést situaci, kdy subjekt sice vhodně zvolí systém zabezpečení, má vypracovaný systém identifikací, autorizací, kontrol, evidencí a pravomocí uživatelů. Ale lidé pracující v tomto systému obcházejí nařízení a nastavení tak, že přílohy k e-mailu přejmenovávají, aby jejich název byl schválen při kontrole v ochranném pásmu a nedošlo k odhalení nepovolených příloh. Po přijetí na svou stanici provedou opětovné přejmenování do původní podoby a problém je na světě. Aplikace takto "protažená" může napáchat značné škody, jejichž důsledky dokáží být velkou komplikací pro řádné fungování organizace.

2.3 Bezpečnostní studie

Celkový pohled na informační bezpečnost zahrnuje rozbor a souhrn všech důležitých činitelů ovlivňujících bezpečnost. Pro většinu malých a středních organizací by měla být bezpečnostní studie prvním krokem ke zdolávání problematiky Informační bezpečnosti.

Cílem studie by mělo být zhodnocení a popis situace v organizaci z hlediska bezpečnosti, nalezení a pojmenování aktiv společnosti, zhodnocení jejich důležitosti a nalezení největší bezpečnostní chyby. Součástí je i návrh základních nápravných opatření. Studie může zároveň posloužit jako podklad pro definování a vyhlášení Bezpečnostní politiky organizace.

2.3.1 Přínosy zpracování bezpečnostní politiky

- již samotný fakt vypracování studie signalizuje vážný zájem organizace zabývat se Informační bezpečností

- komplexní přístup ke všem aspektům bezpečnosti ukáže i na vazby uvnitř společnosti a její fungování
- pohled zvenčí velmi často odhalí a pojmenuje chyby o kterých sice všichni ví, ale „nemluví“ se o nich.

Způsob provedení a získání podkladů ke studii je proveden tak, že organizace vytvoří neformální pracovní skupinu sestavenou se zodpovědných pracovníků jednotlivých oblastí jichž se bezpečnost dotýká a externího zpracovatele studie. Úkolem této skupiny je bořit komunikační bariéry při provádění samotné prohlídky organizace. Informace se získávají formou pohovorů s jednotlivými pracovníky a také vhodně sestavenými dotazníky.

Protože na bezpečnost je nutno pohlížet komplexně, měla by se studie týkat následujících oblastí:

- fyzická bezpečnost
- personální bezpečnost
- bezpečnost IT
- logická bezpečnost
- legislativní otázky

2.3.2 Rozsah bezpečnostní studie

Stanovení rozsahu by mělo být úkolem vedení organizace. Není vhodné se při zpracování studie omezovat jen na některé oblasti, protože bezpečnost je komplexní záležitost. Zužovat zájem na některé vybrané oblasti znamená, že případné problémy nemohou být ani identifikovány. Výsledky této studie mohou být potom použity při stanovení Bezpečnostní politiky organizace a komplexní znalost všech oblastí umožní velmi efektivní přístup při uplatňování této politiky.

Studie popisuje stav bezpečnosti organizace v jednotlivých oblastech. Definiuje aktiva organizace a jejich důležitost pro organizaci a způsob nakládání s nimi. Navrhuje základní ochranná opatření, jejichž použití může přinést okamžitý efekt a výrazné zvýšení bezpečnosti. Velmi často patří do těchto opatření organizační změny a definování rolí a zodpovědností na jednotlivých pozicích v organizaci. Studie je zároveň podkladem pro analýzu rizik při vypracování politiky bezpečnosti organizace.

2.3.3 Cíle informační bezpečnosti

- snížit riziko lidské chyby, krádeže, podvodu nebo zneužití prostředků organizace

- zajistit, aby si uživatelé byli vědomi bezpečnostních hrozeb a otázek s nimi spjatých a byli připraveni se podílet na dodržování politiky bezpečnosti informací v průběhu své běžné práce
- minimalizovat škody způsobené bezpečnostními incidenty a chybami, sledovat je a učit se z nich

2.3.4 Definování aktiv

Aktivem je cokoliv, co má pro organizaci hodnotu. Správné řízení aktiv je pro úspěch organizace životně důležité a je hlavní odpovědností všech úrovní řízení. Aktiva organizace zahrnují:

- fyzická aktiva (např. počítačový hardware, komunikační prostředky, budovy)
- informace (dokumenty, databáze,...)
- software
- schopnost vytvářet určité produkty nebo poskytovat služby – know-how
- pracovní sílu, školení pracovníků, znalosti zaměstnanců, zapracování apod.
- nehmotné hodnoty (např. abstraktní hodnota firmy, image, dobré vztahy atd..)

Většina nebo všechna z těchto aktiv mohou být považována za dostatečně cenná na to, aby si zasloužila určitý stupeň ochrany.

2.3.5 Odhad hrozeb

Aktiva jsou předmětem mnoha typů hrozeb. Hrozba má schopnost způsobit nežádoucí incident, který může mít za následek poškození systému nebo organizace a jejích aktiv. Hrozby mohou mít přírodní nebo lidský původ a mohou náhodné nebo úmyslné. Škoda způsobená incidentem může být dočasné povahy nebo může být trvalá, jako je tomu v případě zničení, nebo nevratného poškození aktiv.

Velikost škody způsobené hrozbou se může při každém výskytu značně měnit – virus může způsobit různě velkou škodu v závislosti na jeho akcích. Takové hrozby mají často přiřazen i stupeň síly, která je s nimi spojena – virus může být destruktivní nebo nedestruktivní [8].

2.3.6 Analýza zranitelností

Zranitelnosti zahrnují slabá místa v systému, která mohou být hrozbou využita a mohou vést k nežádoucím následkům. To jsou příležitosti, které mohou umožnit hrozbě, aby způsobila škodu. Například absence mechanismu řízení přístupu je zranitelnost, která by mohla umožnit výskyt hrozby nežádoucího proniknutí k aktivům a jejich ztrátu.

Analýza zranitelností je prozkoumání slabých míst, která mohou být využita identifikovanými hrozbami. Zranitelnost konkrétního systému nebo aktiva vůči určité hrozbě je vyjádřením o snadnosti, s kterou může být systém nebo aktivum poškozen.

2.3.7 Odhad dopadů

Dopad je důsledek nežádoucího incidentu, způsobeného buď náhodně nebo úmyslně, který má vliv na aktiva. Následky mohou mít podobu zničení určitých aktiv, poškození systému IT, a ztráty důvěrnosti, integrity, dostupnosti, autenticity, individuální zodpovědnosti nebo spolehlivosti. Měření dopadů umožňuje vytvoření rovnováhy mezi výsledky nežádoucích incidentů a náklady na ochranná opatření a četností jejich výskytu.

Kvantitativní a kvalitativní měření dopadů lze docílit např.:

- stanovením finančních nákladů
- přiřazením empirické stupnice síly, např. 1 – 10
- použitím adjektiv z předem definovaného seznamu, např. nízký, střední, vysoký, atd...

2.3.8 Analýza rizik

Riziko je potenciální možnost, že daná hrozba využije zranitelnosti, aby způsobila ztrátu nebo poškození aktiv nebo skupiny aktiv, a tedy přímo nebo nepřímo organizace. Riziko je charakterizováno jako kombinace dvou faktorů, pravděpodobností výskytu nežádoucího incidentu a jeho dopadu. Analýza rizik tedy dále zpřesňuje odhad dopadů v závislosti na jejich četnosti a ukazuje nám místa, kde je nutno aplikovat ochranná opatření a jaké investice na jejich implementaci jsou adekvátní.

2.3.9 Přijetí zbytkových rizik

Rizika jsou obvykle použitím ochranných opatření pouze zmírněna a z toho vyplývá, že existují zbytková rizika. Součástí posouzení, zda bezpečnost odpovídá potřebám organizace je akceptace zbytkových rizik. Rozhodnutí o akceptaci zbytkových rizik musí učinit ti, kteří jsou oprávněni akceptovat dopad výskytu nežádoucích incidentů a mohou autorizovat implementaci ochranných opatření v případě, že zbytková rizika nejsou akceptovatelná.

2.3.10 Stanovení omezení

Omezení jsou obvykle stanovena nebo rozpoznána vedením organizace a jsou ovlivněna prostředím, ve kterých organizace vyvíjejí svou činnost. Některé příklady omezení, která by měla být vzata v úvahu:

- organizační
- finanční
- personální
- právní
- technická

Tyto faktory musí být při výběru a implementaci ochranných opatření vzaty v úvahu. Časem, sociálním vývojem a kulturou organizace se mohou omezení měnit a proto musí být periodicky prováděny revize.

2.4 Rizika

Bezpečnost dat uložených v informačních systémech je v éře internetu snad nejvíce diskutovaným tématem. Často slyšíme o průniku do různých systémů a možná už jste se s tím setkali na vlastním IS.

Zkusím nastínit několik nejzákladnějších a nejobvyklejších způsobů, jak je možné se do systému dostat.

- prolomení hesla hrubou silou
- prolomení hesla sociálním útokem
- hardwarové útoky

2.4.1 Prolomení hesla hrubou silou

Jedním z nejjednodušších způsobů, jak se potenciální narušitel dostane do vašeho systému je uhodnutí hesla. V současné době již existuje natolik dokonalý software, který je schopen během poměrně krátkého časového okamžiku vyzkoušet obrovské množství kombinací znaků (tzv. útok hrubou silou). Kromě toho tyto programy disponují obsáhlým slovníkem, z něhož se generují nejčastější řetězce používané jako hesla.

Můžete si být téměř jistí, že hesla typu: "heslo", "jméno_vaší_přítelkyně" nebo „rok narození“ není žádný zvláštní problém odhalit. Některé systémy, se brání tak, že uživateli, který opakovaně zadá chybné heslo, dočasně zablokuje přístup. Obrana však má výraznou slabinu ve své nevybíravosti – přístup je zablokován každému bez rozdílu.

Takže pokud je nastaveno, že se uživatel smí zmýlit jen třikrát jinak následuje odmítnutí přístupu na 12 hodin, stane se administrátor tím nejúspěšnějším „útočníkem“.

Kdo z uživatelů čte přihlašovací jméno, když je tam pokaždé stejné, že? Avšak stačí, aby se z počítače přihlásil někdo jiný a než si „pravý“ uživatel všimne změny loginu, je mimo hru. Nebo se ve vyplňování jména uklepne. Jenomže nastavit deset omylů a potom odepření na pět minut také není právě vhodné. Na takovém obyčejném úřadu, kde se žije od sedmi do čtyř odpoledne, by takové nastavení dovolilo bez rizika vyzkoušet každý den mimo pracovní dobu 1 800 možností.

2.4.2 Prolomení hesla sociálním útokem

Dalším nebezpečím jsou tzv. sociální útoky, využívající k proniknutí do systému vaši chybu a případně znalosti o vaší osobě. Takže není vhodné jako heslo používat své rodné číslo, jméno manželky za svobodna, svůj oblíbený nápoj a nebo oblíbenou postavu z večerníčku.

Bohaté zkušenosti správců sítí hovoří jednoznačně: není problém zavolat, představit se jako správce sítě, požádat kohokoliv o sdělení uživatelského jména a hesla a dostat správnou odpověď.

Také při návštěvě kanceláří se dost často objevují hesla nalepená přímo na terminálu případně na klávesnici a o vhodnosti jejich výběru ani nemluvě. Jak by mělo tedy heslo vypadat? Nejdůležitější je sám heslo chránit. Tzn. nikam jej nepsat, nikomu nesdělovat, zvláště ne do telefonu a používat různá hesla pro různé systémy. Často se totiž stane, že musíte jedno heslo sdílet s více lidmi.

Zároveň je třeba se mít na pozoru před různými internetovými službami a protokoly. Například HTTP autentifikace, telnet nebo POP3 protokol pro čtení pošty posílají heslo přes síť buď nezašifrované a nebo zašifrované známou, obousměrnou (tj. heslo lze dešifrovat) metodou.

Všechny tyto služby už mají v současné době své bezpečnější varianty, například SSL, SSH a podobně. Velké firmy si najímají lidi, kteří provádí sociální útoky přímo na zaměstnance dané organizace. Kdo své heslo prozradí, má problém.

Druhým důležitým prvkem ochrany je vhodná volba hesla. Heslo by mělo být alespoň 6 - 8 znaků dlouhé a kromě velkých a malých písmen by mělo obsahovat ještě další znaky, jako jsou číslice, interpunkční znaménka a další speciální znaky. Mělo by být také snadno zapamatovatelné, protože tím, že si ho nemusíte nikam napsat, zvýšíte jeho bezpečnost. V žádném případě by heslo nemělo být tvořeno jedním slovem, bezpečná není ani kombinace slova a číslice (např. jirka2).

Oblíbeným, ale dnes již známým trikem je psát na klávesnici heslo o jedno (nebo více) písmenko doprava (a nebo doleva), takže například místo hesla "franta" vznikne "gtsmys". Nejlepší heslo vznikne tak, že si vymyslíte tu nejjobskurnější kombinaci znaků a pak si ji zapamatujete. Lze ale také vytvořit heslo tak, že vezmete první písmena prvních několika slov nějaké básničky, budete střídát malá a velká písmena - například "sPpO,pZI" (oblíbená Skákal pes přes oves).

Také je možné zvolit možnost, že uživateli se při změně hesla vypíše několik variant, které systém vygeneruje a uživatel si musí jednu z nich vybrat. V neposlední řadě je také třeba vědět, jak s hesly nakládá samotný operační systém.

Vzhledem k rostoucí oblibě Linuxu a dalších klonů Unixu na serverech, budu se věnovat právě tomuto operačnímu systému. Ve starších systémech anebo ve špatně nakonfigurovaných systémech, se hesla ukládala do souboru /etc/passwd. Tento soubor měl práva nastavena tak, že jej mohl číst jakýkoliv uživatel. Hesla zde samozřejmě byla uložena v zašifrované podobě - pomocí funkce crypt. Modernější systémy používají soubor passwd pouze k uložení údajů o uživateli a heslo je uloženo v souboru /etc/shadow, který však může číst pouze root (správce) - tím je zaručena větší bezpečnost. I když je funkce crypt nesymetrická tj. ze zakódovaného tvaru nelze zpětně určit původní heslo, je možné zneužít znalosti zakódovaného tvaru k "útku hrubou silou". V současné době se již ke kódování hesel používají bezpečnější algoritmy, např. MD5.

2.4.3 Hardwarové útoky

Využívají k útoku nedokonalosti hardware. Mezi nejznámější patří tzv. sniffing, tj. na síti odposloucháváme pakety, které nám nepatří. Například na jednom z nejrozšířenějších typů sítí Ethernet se data neposílají konkrétnímu počítači, což ani není možné, ale celému segmentu. Pomocí vhodného software tak lze donutit síťovou kartu, aby zachytávala všechny datové pakety, nejen ty určené počítači, kde je instalovaná. V nich je pak možné najít spoustu zajímavých informací, například uživatelské jméno a heslo.

Odposlouchávat komunikaci lze i "napíchnutím se" na kabel mezi počítačem a modemem. K technicky náročnějším odposlechům patří například "odposlech monitoru" - každý monitor vyzařuje silné elektromagnetické pole, které je možno zachytit anebo instalace nějakého záznamového zařízení mezi klávesnici a počítač. Do této skupiny by se dala zařadit i fyzická bezpečnost serveru. Pokud jej nemáte řádně

zabezpečený, můžete mít ochranu jakou chcete, když si někdo počítač odnese anebo si "půjčí" disk, dostane se do něj vždycky.

Ochrana počítače heslem v BIOSu je naprosto nedostatečná, jednak nezabrání vyjmutí disku a navíc lze snadno zrušit resetováním paměti CMOS. I zde však existuje pomoc - některé programy dokáží zašifrovat disk, takže ten kdo nezná heslo, nemá šanci získat jakákoliv data. Pokud však heslo zapomenete, jste bez šance i vy, zachránit data již nedokáže nikdo. Je vidět, že způsobů, jak se někam dostat je opravdu hodně.

V oblasti bezpečnosti informačních systémů tak platí zlaté pravidlo prověřovat, prověřovat prověřené a pro jistotu ještě prověřit to ostatní. S tím vším vám může pomoci bezpečnostní audit nezávislé poradenské autority [8].

3 Integrace podnikových aplikací

Úkolem této kapitoly je odpovědět na tři základní otázky: Proč je nutné integrovat podnikové aplikace, jak fungují a co nabízejí moderní integrační platformy a zda lze využít datových skladů při integračním procesu.

3.1 Proč potřebujeme integrovat podnikové aplikace

Integrace podnikových aplikací (EAI) patří ke stěžejním součástem systémové integrace v českých firmách. Proto také systémoví integrátoři nabízejí na našem trhu pestrou škálu různorodých EAI řešení. Podle agentury Gartner by měly právě tyto standardní EAI platformy nalézt již na konci roku 2008 uplatnění ve 40% středně velkých a velkých organizací po celém světě.

Co je příčinou tohoto optimistického odhadu? Vychází spíše ze zbožného přání dodavatelů a systémových integrátorů nebo z požadavků zákazníků? V čem vůbec může být nasazení EAI prospěšné [7]?

3.2 Nadbytečné náklady

Nákup a provoz informačních systémů představuje pro podniky nemalé náklady. Ty přitom nemají jen hmatatelnou a vyčíslitelnou podobu peněz, které podniky platí za implementaci, správu, údržbu a další služby s nimi spojené. Náklady se navyšují všude tam, kde je třeba pracovat s roztržštěnou strukturou aplikací, kde nejsou účelně spravována podniková data, i tam, kde nedostatky systému způsobují neefektivní řízení podnikových procesů.

Tato situace je charakteristická především pro velké podniky. Vznikala postupným zaváděním různých systémů v různých obdobích fungování firmy. Tyto systémy měly pochopitelně odlišnou kvalitativní úroveň, historický vývoj se také podepsal na jejich následném vývoji a možnosti inovace.

3.3 Nevhodná řešení

Neintegrovaná architektura sebou přináší mnoho duplicit a nekonzistentností v podnikových datech. Pro rozhodování vrcholového managementu je však zapotřebí rychle zajistit spolehlivé informace, vytvářející obraz "jedné nezpochybnitelné pravdy". Jak je ale získat z nekonzistentních dat rozptýlených v různých podnikových aplikacích? Mnoho organizací volí snadné, ale nevhodné řešení tím, že nechá vyvinout jednoúčelové rozhraní mezi podnikovými aplikacemi, z nichž jsou kritická data

požadována. U velké organizace se pak můžeme setkat s desítkami takových rozhraní. Jen jejich údržba může zatěžovat IT rozpočet náklady ve výši stovek tisíc korun ročně.

To má logicky vliv jak na vznik nadbytečných nákladů, tak i na celkovou efektivnost zpracování informací v organizaci. Lze s tímto přístupem vystačit v době, kdy dostupnost kvalitních informací přímo ovlivňuje konkurenceschopnost firmy, kdy rozhoduje její schopnost adaptovat se neustálým změnám podnikatelského prostředí?

3.4 Pružně proti konkurenci

Extrémně vysoké nároky jsou kladeny především na pružné přizpůsobování podnikových procesů, a to samozřejmě za plné podpory informačního systému. Zatímco malá firma může podle potřeby např. změnit způsob řízení výroby či ji rovnou přesunout za lepšími podmínkami, velká korporace se dostává do problému. Je "svázána" jednak vnitrofiremní organizací, jednak daleko rozvinutějšími vazbami k dodavatelům i zákazníkům.

To jsou hlavní příčiny nepružnosti velkých podniků, které ale nakonec flexibilně reagovat musejí, aby na trhu vůči menším podnikatelským subjektům obstály. Z hlediska zabezpečení podnikových procesů informačním systémem jim k tomu může pomoci dlouhodobě budovaná a uplatňovaná informační strategie. Tato strategie by měla mít také jasně vymezené dílčí koncepce zahrnující řízení klíčových podnikových procesů (ERP), vztahů se zákazníky (CRM) a dodavatelských řetězců (SCM).

3.5 Nástup EAI

Vraťme se ale k podnikovým aplikacím, brzdícím rozvoj firmy a generujícím nadbytečné náklady. Nabízí se ideální východisko ze situace - pokrýt všechny podnikové procesy moderním integrovaným systémem. Bohužel v praxi lze toto řešení uplatnit jen výjimečně. Představuje totiž značné náklady promítnuté do realizace složitého projektu a nenavrácené investice do původních dílčích systémů. Značná rizika by spočívala také v samotném zadání rozsáhlého projektu. Za mnoho měsíců implementace by totiž nemuselo odpovídat rychle se měnícím požadavkům organizace. Ukazuje se tedy, že nejvhodnějším způsobem je využití moderní EAI platformy. Co ale kromě již zmíněných obecných problémů určuje poptávku po EAI?

3.6 Ekonomický pohled

Prvořadým úkolem ekonoma je snižovat a kontrolovat náklady. V oblasti IT jde zejména o náklady na vlastnictví (TCO) a jejich součást - náklady na provoz (RTC).

Proč by měl ekonom podporovat nasazení EAI? Hlavní důvod spočívá v umožnění návratnosti investic do stávajících podnikových aplikací (ROI). Z ekonomického hlediska je důležitá také centralizace zpracování dat, která může určit hranice a vazby mezi aplikacemi. Pak je možné lépe měřit jejich provozní charakteristiky a finanční náročnost. Dalším faktorem podporujícím poptávku z pohledu ekonoma je úspora v oblasti lidských zdrojů. Roztříštěnost původních aplikací totiž vede nadbytečným nákladům na obsluhu koncovými uživateli. Ty vznikají především velkou pracností obsluhy, vysokou chybovostí a značnými nároky na školení.

Kromě tradičních ukazatelů lze použít také indikátor hodnotící náklady na změnu, resp. přizpůsobení informačního systému novým podmínkám (CTC). Jedná o náklady, které musí podnik vynaložit na vylepšení či změnu určitého procesu, a to včetně položek, jako jsou náklady na dodatečný hardware, nové licence, služby konzultantů atd. CTC slouží primárně k tomu, aby bylo možné vyhodnocené náklady porovnat s budoucími přínosy této změny. Na základě tohoto ukazatele se pak lépe rozhoduje o předpokládané investici [1].

3.7 Z pohledu procesního řízení

Vedoucí pracovníci klíčových podnikových úseků, jako je výroba, obchod nebo logistika, jsou postaveni před problém rychlého zavádění nových metod řízení či optimalizaci stávajících procesů. Integrace podnikových aplikací na bázi standardní EAI platformy jim přitom nabízí možnost pružně reagovat na změny vnějších i vnitřních podmínek, ať už z hlediska legislativy, změn situace na trhu, personálních změn apod. Flexibilita je dále podporována spouštěním klíčových procesů napříč všemi integrovanými aplikacemi. Velmi přínosná je také možnost sledování procesů (BAM). Manažeři klíčových procesů budou mít zájem rovněž na zlepšené podpoře týmové práce. EAI předpokládá mj. nasazení jednotného intuitivního pracovního prostředí - portálu. Uživatel díky portálové technologii v podstatě vůbec nepozná, že se řešením svých úloh v rámci procesu pohybuje v různých aplikacích. Pro uživatele je rozhodující také možnost poskytování informací potřebných k rozhodování v reálném čase a dostupnost analytických funkcí systému.

3.8 Co rozhoduje v IT oddělení

IT management nahlíží na EAI platformu přes její technologické řešení. Přitom by se však měl opírat o jasně deklarovanou podnikovou a IT strategii a o požadavky všech vedoucích pracovníků. K jasným preferencím IT oddělení z hlediska nasazení

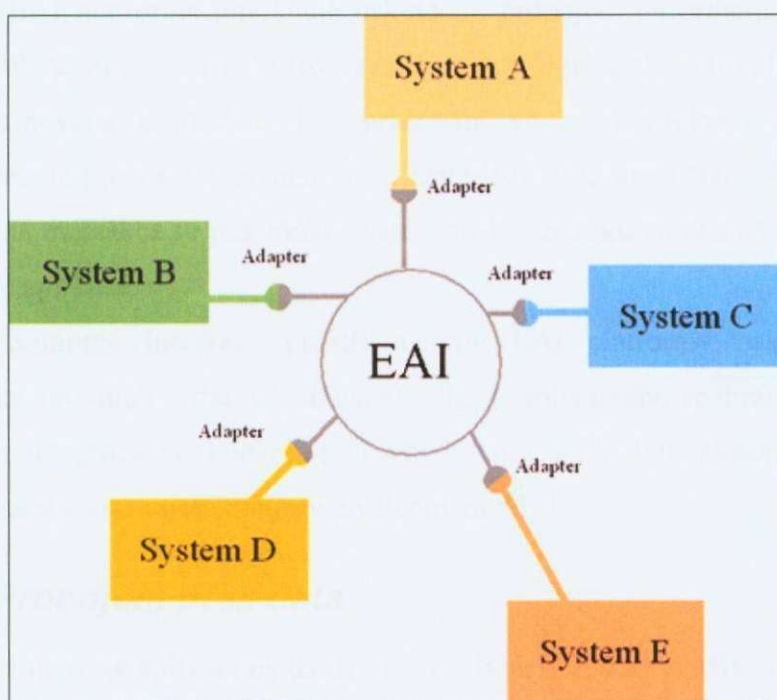
EAI platformy pak patří dosažení konzistence dat, existence jednoho univerzálního úložiště a schopnost vytvářet jednotné prostředí pro přenos dat i aplikací. Důležité je především zajištění spolehlivých komunikačních kanálů a služeb pro přenos zpráv a to včetně jejich kvalitního zabezpečení a ochrany. Výhodou je také připravené rozhraní, zejména pak do podnikového ERP či systémů integrovaných v dodavatelském řetězci. Pro podnikání v dodavatelských řetězcích je rozhodující také podpora komunikačních protokolů pro elektronickou výměnu dat (EDI). IT oddělení ocení mj. integrované jednotné vývojové prostředí, kvalitní správu metadat pro řízení technologických vrstev EAI a jednotnou sadu nástrojů na jeho správu a údržbu.

4 Jak fungují a co nabízejí moderní integrační platformy

Možnosti integrace podnikových aplikací se vyvíjejí řadu let společně s rozvojem nových technologií a změnami požadavků zákaznických organizací. Z technologického hlediska zasáhl do tohoto procesu nejvýrazněji nástup osobních počítačů, zavádění architektury klient/server a využití internetu v podnikové sféře. Požadavky zákazníků se měnily společně s rostoucí konkurencí, globalizací trhu a rozvojem podnikání v rámci dodavatelských řetězců.

4.1 Otázky pro manažery

Integraci podnikových aplikací (EAI) můžeme charakterizovat jako propojení původně nezávislých dílčích řešení či informačních systémů, které jsou vzájemně nekompatibilní a jejichž správa a údržba probíhá nezávisle (viz. obr. 4.1). EAI jako jednotná aplikační platforma pak logicky musí obsahovat soubor nástrojů a technologií, které umožní kompaktní správu a efektivní spolupráci dopsud nezávislých aplikací.



Obr. 4.1 - Koncepce EAI

Může nám EAI nabídnout i další služby? Nejde přece jenom o náklady na implementaci, provoz a údržbu, trápí nás často celková efektivita zavádění nových

aplikací a procesů. Nedokážeme posoudit, jak jsou tyto procesy monitorovány a kolik na ně vynakládáme lidských a systémových zdrojů. Chybí nám konkrétní informace o tom, jak dlouho např. trvá vyřízení obchodního případu. A pokud bychom takovouto informaci získali, dokážeme rychle dané procesy změnit podle aktuálních požadavků?

4.2 Kudy nelze jít

Začněme ale nejprve u způsobů integrace podnikových aplikací. Existují v podstatě dva. Ten první, se nazývá "point-to-point" - každý s každým. Spočívá ve vytváření účelových propojovacích řešení zabezpečujících synchronní komunikaci mezi aplikacemi. Tento přístup je v praxi doposud hojně využíváný, avšak není příliš efektivní. Generuje nadbytečné náklady na vývoj každého jednotlivého komunikačního řešení a předpokládá značnou pracnost s rozdílnými komunikačními protokoly či zdrojovými kódy nestandardních aplikací. Dále také počítá s připraveností aplikací na synchronní komunikaci. Pokud však aplikace dostupná není, transakce nemůže být provedena.

4.3 Jak funguje EAI řešení

EAI platforma umožňuje uskutečnit propojení na principu middlewaru. Slouží jako sdílené místo, na něž jsou zasílána data z jednotlivých aplikací a kde jsou také transformována a předána ke zpracování ve srozumitelném formátu. EAI řešení zabezpečuje přenos dat asynchronně. Data jsou totiž umístěna "ve frontě" middlewaru. Příslušná transakce se pak může uskutečnit bez nároku na okamžité propojení zdrojové a cílové aplikace.

Samotná integrace prostřednictvím EAI platformy pak může probíhat na několika úrovních - datové, uživatelského a aplikačního rozhraní a obchodní logiky. Využití integrace na konkrétní úrovni by pak mělo být odrazem potřeb zákaznické organizace a vlastností integrovaných aplikací [7].

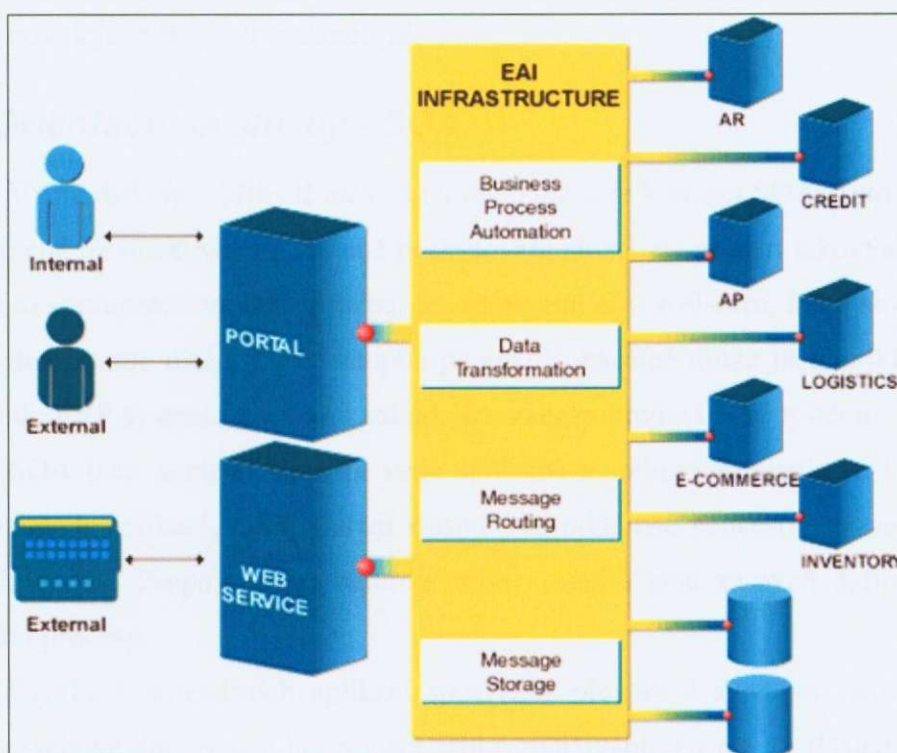
4.4 Propojení přes data

Integrace aplikací na datové úrovni (viz. obr. 4.2) využívá úložišť dat a možností jejich přesunu. Přitom v podstatě ignoruje existenci aplikací jako takových. Tento přístup nemusí být na škodu, neboť většina aplikací funguje obdobně - ukládá data do relačních databází. Data z jedné databáze jsou pak za pomoci ETL nástrojů automaticky čištěna, transformována a uložena v požadované struktuře do databáze sloužící jako datové úložiště jiné aplikace. Jde o docela dobré a rychlé řešení s jasně čitelnými

přínosy spočívající zejména v úspoře nákladů v porovnání s ostatními způsoby integrace. Hodí se také k budování operačních datových skladů (ODS). Může však narazit na obtíže s udržováním velkého množství databázových tabulek. Pokud od EAI požadujeme vysokou flexibilitu a schopnost práce v reálném čase, pak integrace na datové úrovni není příliš šťastné řešení [3].

4.5 Uživatelské rozhraní a portál

Zatímco "datový přístup" ignoroval existující aplikace, propojení přes uživatelské rozhraní jde přesně opačným směrem. Snaží se automatizovat práci uživatele a to tak, že odpovědi systému na vznesený požadavek jsou výsledkem simulací uživatelského postupu. Jedná se o způsob využíváný především tehdy, kdy je potřeba integrovat velmi staré aplikace, u nichž není k dispozici zdrojový kód, a kdy nelze využít jiného integračního postupu. V jiných případech by ale toto řešení bylo velmi neefektivní. Je totiž závislé na neměnnosti aplikace, s čímž můžeme u modernějšího softwaru jen velmi těžko počítat.



Obr. 4.2 - Architektura EAI

K integraci přes uživatelské rozhraní lze jistě zařadit také moderní trend nasazování portálových technologií - jednu z klíčových součástí EAI řešení. Portál však neslouží primárně k tomu, aby zabezpečoval výměnu dat mezi aplikacemi. Jeho úkolem

je sjednotit uživatelské rozhraní a zabezpečit intuitivní přístup k aplikacím, aniž by byl uživatel zatěžován jejich sledováním v rámci svého podnikového procesu.

4.6 Příliš těsné propojení

Při integraci je možné využít také aplikačního programového rozhraní (API), které poskytuje výrobce konkrétní aplikace. Pomocí API lze přistupovat jak k datovým zdrojům, tak k obchodní logice jednotlivých aplikací. Propojení pomocí API se využívá u složitých, nestandardních aplikací. Je však zcela závislé na výrobci daného API. Integrace na bázi obchodní logiky znamená způsob zasahující do struktury stávajících podnikových aplikací. Cílem propojování na této úrovni je sdílet klíčové postupy sloužící při řízení celé organizace. Operace prováděné různými aplikacemi pak budou vykonávány stejně. Tento přístup také zjednodušuje správu a aktualizaci jednotlivých komponent. Na druhé straně je také nositelem mnoha rizik. Především vytváří velmi těsnou vazbu mezi aplikacemi a vzájemnou závislost. Ve své podstatě je příliš složitý, nákladný a pracný pro vývojáře či servisní podporu. Podobná rizika přináší integrace na úrovni dat, uživatelského i aplikačního rozhraní. Předpokládá totiž sdílení interních charakteristik jednotlivých aplikací [2].

4.7 Orientace na služby - SOA

Východiskem z příliš těsné a složité integrace je koncept SOA. Tato architektura je zaměřena na opakované a sdílené poskytování služeb za použití takových standardů, které tuto spolupráci umožní. Služba, je autonomní část softwaru, která slouží k plnění přesně definované úlohy a je dostupná po síti. Konkrétně může jít například o zadání faktury do ERP systému nebo získání údajů o zákazníkovi z CRM systému.

SOA jako ucelený koncept vede společně s webovými službami k vývoji tzv. kompozitních aplikací, které slučují dosud dvě oddělené součásti - vývoj aplikací a jejich integraci. Propojováním heterogenním systémů jsou zároveň definovány nové obchodní procesy.

Tvorba kompozitních aplikací spočívá v převedení stávající funkcionality do podoby webové služby a v koordinaci jejího využívání. To má za důsledek výraznou redukci nákladů na vývoj a provoz systému a rychlé zavádění nových služeb do praxe. Samotná koordinace webových služeb pak představuje asynchronní i synchronní formu komunikace na úrovni, která je pro daný přenos dat nejvhodnější. Pro popis těchto nově definovaných procesů se používá standardní jazyk (BPEL), přijatý předními IT dodavateli jako standard.

4.8 Co nabízí moderní EAI

Výběr EAI platformy, která nám pomůže vyřešit otázky položené na začátku, závisí tedy na její schopnosti využít SOA a webové služby, vytvářet a integrovat nové procesy. Významný podíl na EAI představují rozsáhlá komponentová řešení. Na českém trhu je reprezentují zejména platformy SAP NetWeaver a Oracle Integration, ve světě pak kupříkladu webMethods Fabric.

Základním stavebním kamenem těchto řešení jsou otevřené standardy plně spolupracující s jinými platformami jako je např. Microsoft.NET. Jednotlivé komponenty EAI jsou pak orientovány vždy na specifický problém integrace. Nasazují se např. za účelem integrace různorodých prostředí, aby zajistily rychlý přenos dat a dokumentů (Oracle InterConnect). Nelze opomenout ani podporu vrcholového rozhodování. Může fungovat buď na základě využití nástrojů Business Intelligence, tedy na hloubkových analýzách dat (SAP BI), nebo může vycházet z kontinuálního sběru dat ze všech integračních komponent a jejich přiřazování definovaným ukazatelům (KPI). Pomocí KPI pak mohou zodpovědní manažeři sledovat chod celého podniku (OracleAS Integration BAM).

4.9 Specializované platformy

Pro fungování podniku v dodavatelském řetězci je podstatná podpora B2B komunikace, resp. konkrétních standardů sloužících k výměně dat (EDI, XML atd.). Na tento integrační problém jsou orientovány produkty, jako je např. Microsoft BizTalk Server, GE Global eXchange Services nebo TradeXpress Enterprise. V rámci dodavatelského řetězce je standardizace elektronické komunikace mimořádně důležitá. V některých případech, jako je např. komunikace centrály s distribučním centrem nebo s pobočkami, je výhodné její přenesení právě do platformy EAI.

Na druhé straně existuje skupina EAI platform, které kladou důraz např. na schopnost automaticky vytvářet aplikace se specifickou funkcí na základě integrace stávajících aplikací. Silnými nástroji pro modelování podnikových procesů a následný vývoj aplikací disponují např. Versata Process Logic Engine nebo TIBCO Software [11].

4.10 Nabídka pro všechny

K zajímavým EAI platformám patří Ensemble od společnosti InterSystems. Ensemble sám o sobě tvoří samostatnou skupinu EAI řešení. Jde o jednoduchý produkt bez

výrazného rozčlenění do specializovaných modulů. Zatímco mnohé ostatní produkty vznikly postupným propojováním původně samostatných úzce zaměřených řešení (např. IBM WebSphere), Ensemble byl navržen jako ucelená platforma opírající se o postrelační databázový stroj Caché. K jeho hlavním konkurentům patří rozsáhlá komponentová řešení, jako jsou SAP NetWeaver nebo Oracle Integration.

Všechny tři skupiny EAI platforem si pak navzájem konkurují nabídkou speciálních nástrojů umocňujících jejich praktické využití v podnikové architektuře. Jde především o podporu podnikového portálu, mobilních řešení a možnost automatické identifikace (čárové kódy i RFID). Moderní EAI řešení si dnes nedovedeme představit také bez kompozitních aplikací, které dokáží nahradit nepraktická rozhraní mezi jednotlivými softwarovými systémy a bez rozsáhlé sady adaptérů pro napojení podnikových aplikací, jako jsou Siebel nebo SAP.

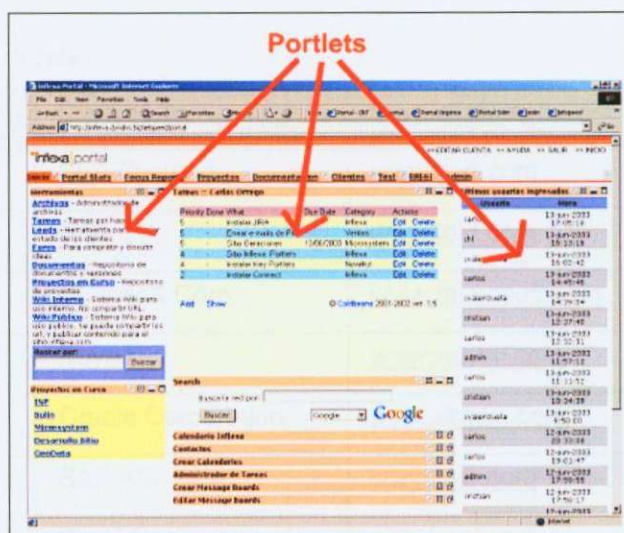
5 Portály

Portálová řešení a technologie dnes mají značný dopad na provoz podnikových informačních systémů. Firmy se jednoznačně odklánějí od tradičních aplikací vytvořených pro uživatelské počítače.

Například pro přístup do ERP systému žádají, aby bez potřeby jakékoliv instalace na své straně měli přístup ke všem podnikovým i externím aplikacím z prostředí webového prohlížeče. Portál je webovou aplikací, která zpřístupňuje funkčnost informačního systému a zprostředkovává pohled na jeho databázi. Že se jedná o webovou aplikaci, má hned dvě výhody. Stačí si spustit internetový prohlížeč a všechny poskytované služby jsou uživatelům dostupné. Druhou výhodou je nezávislost prohlížeče na operačním systému, a dokonce i hardwaru.

5.1 Architektura portálu

Každý portál je tvořen třemi prvky: rolemi, portlety a šablonami. Role definují přístupová práva jednotlivých uživatelů podle jejich postavení nebo funkce v podniku. Na základě práv uživatel získává oprávnění přistupovat k datům, schvalovat dokumenty, navštěvovat fóra, využívat služeb a nástrojů pro spolupráci apod. Portál má podobu několika pracovních prostorů, ve kterých jsou publikovány požadované informace. Poskytována jsou nejen pasivní data, ale také aktivní, která jsou generována aplikacemi nebo systémy (ERP, CRM). Informace jsou zobrazovány prostřednictvím portletů (viz. obr. 5.1), které vypadají na webové stránce jako malé rámečky. Podle profilu uživatele zajišťují funkce nad daty, ke kterým má daný uživatel přístupová práva. Každý portál nabízí bohatou sadu standardních portletů. Portlety jsou sdružovány do šablon. Mohou být sestaveny podle jazyka uživatele, pracovní skupiny, ke které náleží atd. Šablony představují kostru portálu [6].



Obr. 5.1 - Struktura portálu - portlety

5.2 Klíčové rysy portálu

Základní funkcí je poskytování informací z různých zdrojů svým uživatelům, jejich seskupování a třídění pro další použití podle témat, a to prostřednictvím jednotného snadno použitelného rozhraní, což výrazně umožňuje zvýšit efektivitu jednotlivých pracovních stanic. Samotné předávání velkého množství informací by příliš užitečné nebylo bez možnosti přizpůsobení. Aby portál vyhověl požadavkům společnosti a zároveň zajišťoval neustálý přístup k aktuálnímu obsahu i službám, musí splňovat také požadavky na úpravu podle zájmů a potřeb jednotlivých uživatelů (např. vzhled portálu, jazyk, eliminace nechtěného obsahu apod.). Portál také pomáhá podle jasných kritérií rychleji najít informace, aplikace a služby bez ohledu na to, kde se nacházejí. Zjednodušuje spolupráci uživatelů v rámci komunikace uvnitř podniku i v rámci pracovní skupiny tvořené zástupci několika společností, která je sestavena pro spolupráci na určitém projektu. Pouze jediným přihlášením portál zabezpečuje automatické přihlašování (Single Sign On) pro potřeby přístupu k nejrůznějším externím zdrojům. Podnikový portál je dynamické prostředí propojené se strukturou a růstem podniku, proto musí být schopen rychle reagovat na změny počtu uživatelů, typu služeb nebo oddělení společnosti [13].

5.3 Bezpečnost

Tabulka 1 - Přehled významných portálových řešení

Název produktu	Dodavatel	www stránky
BEA WebLogic Portal	BEA Systems	www.bea.com
IBM WebSpherePortal	IBM	www.ibm.com
Microsoft Office Sharepoint Portal Server	Microsoft Corp.	www.microsoft.com
Novell Portal Services	Novell	www.novell.com
Oracle 9i Application Server Portal Rel.2	Oracle Corporation	www.oracle.com
SAP Enterprise Portal	SAP AG	www.sap.com
Sun One Portal Server	Sun Microsystems Inc.	www.sun.com
Sybase Enterprise Portal	Sybase Inc.	www.sybase.com

Důležitou vlastností podnikových portálu je ošetření přístupových práv, přihlašování a dalších aspektů z oblasti bezpečnosti. Bezpečnostní opatření mohou řídit a kontrolovat jak přístupy zaměstnanců, tak zákazníků a partnerů. Informace

publikované na portále můžeme rozdělit na všeobecně přístupné široké veřejnosti (anonymní uživatel) a na informace, které vyžadují identifikaci uživatele. Přístup k takovým informacím je umožněn na základě uživatelského jména a hesla. Velice citlivé údaje je možné zabezpečit také pomocí klientského certifikátu. Pokud by se dostaly do nepovolaných rukou, následky zcizení jsou potom nevyčíslitelné. Proto je třeba bezpečnosti informací a zabezpečení portálového řešení věnovat velkou pozornost. Nezapomínejme také na rušení účtů po odchodu pracovníků.

5.4 Portál jako intranet

Intranet je charakterizován jako lokální podniková síť, která využívá internetové standardy. Interním uživatelům takové sítě je umožněno přistupovat k internetovým zdrojům a získávat z nich informace, naproti tomu externím vstup do intranetu bez přístupových práv není povolen. Co by měl intranet neboli zaměstnanecký portál - B2E (Business to Employee) mít? K základním aplikacím, které ke své práci potřebuje každý uživatel, patří zejména e-mail, firemní adresář, katalog zboží, sdílené kalendáře, sdílené úkoly, správa projektů, přehled podnikových norem, standardů a pokynů. Přístup k dalšímu obsahu zaměstnaneckého portálu je určen individuálními požadavky konkrétního uživatele a podle jeho role ve vztahu k organizaci. Například role prodejce obsahuje také přístup k příslušným aplikacím CRM (řízení vztahů se zákazníky).

5.5 Expanze za hranice

Pomocí stejných technologií je možné rozšířit vnitropodnikový intranet o další skupiny uživatelů za hranicemi firmy. První skupinou externích uživatelů jsou důležité odběratelé, dodavatelé, partneři atd. Této skupině je umožněn přístup k vybraným službám, informacím a dokumentům interních informačních systémů společnosti, které jsou důležité a podstatné pro fungování dodavatelsko-odběratelských vztahů nebo pro spolupráci. Tuto část portálu označujeme jako partnerský portál B2B (Business to Business). Součástí extranetu může být i internetový obchod. Tato část podnikového portálu je přístupná široké veřejnosti - zákaznický portál B2C (Business to Consumer).

5.6 Mobilní přístup

Kromě klasického přístupu pomocí počítače a internetového prohlížeče je možno přistupovat k portálu pomocí mobilních zařízení. Musí však splňovat jedinou podmínku, aby zařízení obsahovalo prohlížeč. Příkladem mohou být mobilní telefony s technologií WAP, kapesní počítače (PDA) atd. Automaticky je rozpoznán typ prohlížeče mobilního

zařízení a je přiřazen příslušný obsah pro tento prohlížeč. Funkcionalita mobilního přístupu je standardní součástí portálu, a není tedy nutná instalace žádného dalšího softwaru.

5.7 Přínosy a rizika

Nasazení a dlouhodobé budování podnikových portálů přináší především zefektivnění podnikových procesů uvnitř firmy i směrem k partnerům a zákazníkům, snížení provozních nákladů a zkrácení potřebného času. Portály přináší také úsporu nákladů při správě pracovních stanic a jednodušší administraci celého systému včetně správy oprávnění, centrální správy uživatelů a možnosti integrovaného přístupu k bezpečnostní politice společnosti. V neposlední řadě je v rámci portálů často využívána správa dokumentů (dokument management system) včetně jejich klasifikace, vyhledávání a společného sdílení uživateli.

Mezi největší rizika implementace portálu patří podcenění komplexnosti obsahu projektu a často měnící se požadavky. Důležité jsou také výkonostní testy s následnou optimalizací výkonu portálu podle předpokládané zátěže s ohledem na počet současně přihlášených uživatelů a zpracovávaných požadavků. Významným rizikem také může být podcenění marketingového plánu pro zviditelnění nového portálu [14].

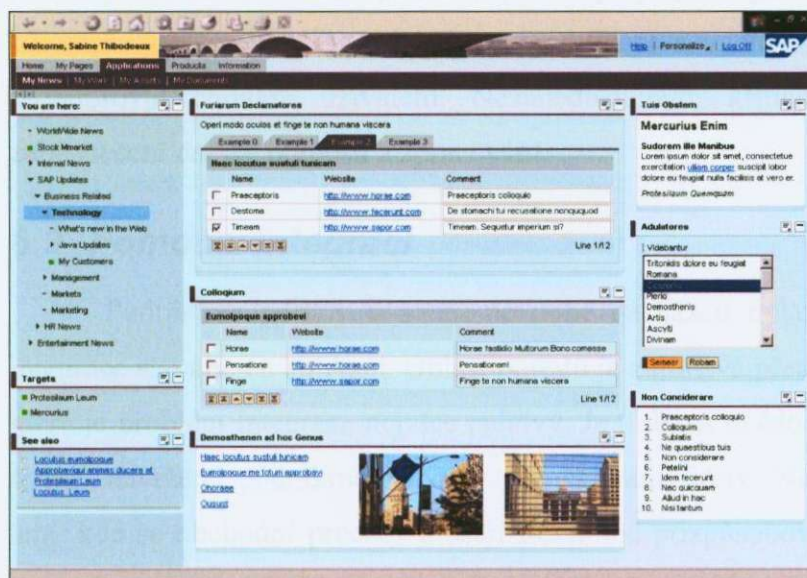
6 Vliv portálových řešení na provoz podnikových informačních systémů

6.1 Od historie k aktuální nabídce

První portály fungovaly jako křižovatky, které své návštěvníky naváděly na stránky, kde se požadované informace nacházely. Nejprve nabízely pouze vyhledávání podle seznamu odkazů na dostupné stránky - katalogové vyhledávání. K němu později přibýlo fulltextové a různé podoby rozšířeného vyhledávání. Postupem času se pohled na internetové portály změnil, což se také odrazilo v jejich nabídce. Portály začaly poskytovat bezplatnou elektronickou poštu a vystavování webových stránek. Nakonec se přidaly zprávy a informační služby (předpověď počasí, kurzy měn a akcií, programy televize, horoskopy a další). Taková záplava informací působila značně nepřehledným dojmem. Tato situace přinesla uživateli možnost vlastní úpravy obsahu webové stránky,

může si navolit informace a služby, které jej zajímají a které si nepřeje zobrazit.

Odtud už byl jenom malý krůček k podnikovým portálům. Jak je vůbec možné, že se portály staly oblíbeným nástrojem v podnikové sféře? V podnicích existuje mnoho skupin uživatelů



Obr. 6.1 - SAP Enterprise Portal

s různými informačními potřebami a právě uzpůsobení obsahu podnikového portálu umožňuje, aby každý uživatel měl na jednom místě zrovna ty informace a služby, které potřebuje ke své práci. Uživatel se tak při hledání relevantních informací nemusí probírat záplavou zbytečných dat a může se více věnovat své vlastní práci [5].

6.2 Určení kritéria úspěchu

Jaká jsou kritéria úspěšnosti budování podnikových portálů? Nejprve je nezbytné dobře naplánovat celý projekt (rozsah, požadavky, zabezpečení, atd.). Základním kritériem úspěšnosti je dostupnost portálu všem jeho uživatelům a jeho spolehlivost, ať už k němu přistupují pomocí svého počítače nebo pomocí některého z mobilních zařízení. Portál poskytuje uživatelům velké množství informací z různých zdrojů, v různých úpravách, s různou dobou platnosti. Je proto důležité, aby byly vytvořeny metody, které definují a popisují postupy publikování portletů na portálech. Klíčovým požadavkem každého portálového projektu je jednoduchá a rychlá integrace existujících podnikových a externích aplikací. Předpokladem integrace aplikací do portálu je jejich vytvoření na principech vícevrstvé architektury a podpora jednotného přihlašování.

Dalším kritériem je již zmiňované adresné poskytování služeb a informací, které uživatel skutečně potřebuje. Běžnou praxí je rozdělení uživatelů do různých skupin s podobnými informačními požadavky. Skupiny jsou pak základem pro vytvoření uživatelských profilů. Pro následnou modifikaci a vytváření nových profilů je třeba monitorovat chování uživatelů. Nezanedbatelným kritickým faktorem je otázka zabezpečení dat při přenosu a zpracování.

6.3 Pomoc s integrací

Podnikové portály v současné době nacházejí uplatnění především v oblasti integrace stávajících aplikací. Oblast portálů je zajímavá především pro větší firmy, pro které je problém integrace nejvíce palčivý. Je třeba si uvědomit, že nemohou zachránit špatně navržené podnikové procesy a fungování firmy. Největší uplatnění nacházejí tam, kde se obchodní procesy musejí flexibilně přizpůsobovat změnám na trhu, ať už tyto procesy probíhají uvnitř společnosti nebo celým dodavatelsko-odběratelským řetězcem.

6.4 Propojení s partnery

Kdy vzniká potřeba firem zabývat se integrací aplikací? Většinou je vyvolána nutností propojit více interních systémů s aplikacemi obchodních partnerů nebo zákazníků, integrací informačních systémů poboček firmy, případně fúzujících společností. Dalším důvodem může být implementace např. CRM systémů, kdy je třeba sdílet data jiných aplikací.

6.5 Webové služby

Webové služby (Web Services) jsou novým standardem a usnadňují komunikaci a integraci mezi dvěma a více aplikacemi. Přechod z architektury klient/server přes webové orientované aplikace k webovým službám byl součástí postupného vývoje technologií, které vytváření těchto služeb umožňují. V rámci podniku mohou vzájemně propojit různorodé informační systémy, které jsou součástí podnikových procesů. Využívají se pro dynamické vytváření obsahu ze zdrojů (externích a interních) a zpřístupňují tento obsah na podnikové portály.

The screenshot shows the SAP Employee Self-Service interface. Annotations highlight four levels of personalization:

- 0. úroveň přizpůsobení : Podnikový vzhled** (Company Look): Points to the top navigation bar and SAP logo.
- 1. úroveň přizpůsobení obsahu: Má Role** (My Role): Points to the 'Employee' role-based menu.
- 2. úroveň přizpůsobení obsahu: : Má Stránka** (My Page): Points to the 'Hire' button in the bottom navigation bar.
- 3. úroveň přizpůsobení obsahu: Má iViews** (My iViews): Points to the 'Organizational Change' iView.

Personnel number	Name	Organizational Unit	Position	Cost Center	Cost center text
03100087	Mr. Jeremy Davidson	Treasury	Manager of Treasury	0000022100	Finance & Admin
00901144	Mr. Sam Davidson	Large Account Sales	Manager Sales - Large Accounts	0000032000	Marketing
00930155	Mr. Tony Davidson	Western Region Sales	Manager Sales - West	0000032000	Marketing
	Thomas Davidson				

Obr. 6.2 - Možnosti přizpůsobení portálu

Co tedy doporučit společnostem, které se chystají budovat podnikový portál? V první řadě nepodcenit přípravné práce projektu a zvýšenou pozornost věnovat analytické části. Od počátku je třeba vědět, co od portálu můžeme očekávat a zda jsou požadavky splnitelné. Dobře naplánovaný projekt a dodržení všech kroků, které stanoví metodologie, jsou základem úspěchu každého projektu.

7 Využití CRM v energetické firmě

O CRM systémech se před několika lety začalo hovořit také v souvislosti s energetickým průmyslem. Je možné, aby toto "guru řešení" pro řízení vztahů se zákazníky trvale zapustilo i kořeny v odvětví, marketingem do nedávné doby ještě vůbec nepoznamenané?

7.1 Všeobecné souvislosti

Již hodně času uplynulo od doby, kdy se v běžně používané české mluvě zabydlel pojem CRM (Customer Relationship Management). O chvíli později jsme dokonce pochopili jeho význam, podstatu a přínosy. Postupně se pojem CRM rozšiřoval z obecného kontextu do konkrétních slovních spojení a začli jsme ho používat spolu s určitými odvětvími českého průmyslu, např. jako CRM v bankovníctví, telekomunikacích a dokonce i ve spojení se státní správou (což v českých luzích a hájích může vyvolat údiv na tváři). Dalším průmyslem, kde se CRM (předpokládejme, že CRM chápeme jako způsob myšlení, konání, blíže zaměřenou a jistým způsobem i unikátní strategii každé firmy, ne jako pouhý software) začal prosazovat, byla i energetika (hlavně elektrická energie a plyn).

Využití CRM v energetice ale předcházela náročná privatizace zainteresovaných firem, následná liberalizace trhu a v neposlední řadě cenová deregulace. Všechny tyto procesy jsou navíc stále živé, pokračují a ubírají se směrem, který mnohdy laikovi nemůže být ani jasný. V pozadí je navíc nutno vnímat zdlouhavé novelizace na poli příslušných zákonů - můžeme toto komplexně považovat za boření monopolistické struktury a stavbu struktury co nejvíce připomínající tržní vztahy.

Nyní se podrobněji podívejme na současný stav energetického průmyslu ve spojení se vztahem k zákazníkovi – CRM [12].

7.2 Kdo implementuje co

Díky rozhodnutí o přeměně energetického monopolu v tržní prostředí (spíše okolím vynuceným) se v energetickém průmyslu objevilo mnoho nových subjektů věnující se nákupu surovin, výrobě elektrické energie, distribuce plynu či elektrické energie jako i samotní prodejci těchto produktů koncovým zákazníkům (nebo dalším zprostředkovatelům). Jenže toto je změna do jisté míry pouze strukturální. Změna, která by přinášela výhody pro koncové zákazníky plynoucí z definice konkurenčního prostředí jako takového, spočívá ve způsobu chování se ke svým zákazníkům. Nově

vznikající firmy nebo firmy rozšiřující svou působnost z jiných konkurenčně založených odvětví do odvětví energetického mají s tímto přístupem menší problémy, než firmy doposud v energetice působící. Pro ně je mnohdy představa nutné změny chování ke stejnému zákazníkovi velice těžká, což je ovšem jeden ze základních pilířů CRM strategie.

I když by se všechny firmy působící s tímto nově konkurenčně založeným odvětvím měly začít chovat tržně a přání zákazníka by pro ně mělo být "zákonem", ne vždy tomu tak samozřejmě bude. Mnohé firmy, jako jeden z možných konkurenčních nástrojů v boji o zákazníka použijí CRM. Vzhledem k tomu, že energetika je průmysl velice lukrativní, mohou si firmy peníze do investic tohoto typu jistě dovolit. Záměrně jsem použil slovo investice, protože desítky miliónů korun utracené za implementaci CRM řešení musí být chápány jako investice. Pomiňme pohled ze strany účetnictví, kde se při troše dobré vůle dají stejné věci vykazovat různě a podívejme se na tuto investici z pohledu marketingově-strategického: jednoznačně se nám tato investice musí vrátit buď v podobě tržního podílu, zvýšeného počtu zákazníků, zvýšených tržeb, zvýšeného billingu na jednoho zákazníka či jiným dalším směrodatným a věrohodným ukazatelem, který firma sleduje a je pro ni důležitý.

Liberalizace (její zjednodušený harmonogram viz. tabulka) vrhla na trh jako celek, novou energii v podobě boje o zákazníky a v tomto boji se jednotlivé firmy rozhodly používat různé CRM řešení ve víře, že právě tyto řešení budou pro jejich firmu ty pravé a pokud možno ještě lepší než používá konkurence. Pomiňme současný stav procesu implementace u jednotlivých firem, stejně jako technické možnosti jednotlivých řešení (výhody a nevýhody jednotlivých řešení by totiž vydaly na více než jednu další práci - a ani pak by výsledek nebyl zaručen) a krátce shrňme pro jaké řešení se níže uvedené firmy rozhodly.

Firmy působící na českém energetickém trhu si díky dosavadního výsledku privatizace můžeme rozdělit do několika skupin, reprezentující buďto jejich majetkové propojení nebo dočasnou volnost, popř. dočasné přímé majetkové nezařazení ani do jedné ze vzniklých skupin.

Tabulka 2 - Harmonogram liberalizace energetického trhu v ČR, [20]

Od 1. ledna 2002 jsou oprávněnými zákazníky koncoví zákazníci, jejichž spotřeba překročila hodnotu 40 GWh. Takových subjektů je na českém trhu přibližně sedmdesát.
Od 1. ledna 2003 jsou oprávněnými zákazníky koncoví zákazníci, jejichž spotřeba překročila hodnotu 9 GWh. Tyto podmínky splňovalo přibližně 400 subjektů (tj. asi 33 procent českého trhu s elektřinou).
Od 1. ledna 2005 jsou oprávněnými zákazníky všichni koncoví zákazníci, jejichž spotřeba elektřiny překročila hodnotu 100 MWh.
Od 1. ledna 2006 jsou oprávněnými zákazníky všichni koncoví zákazníci, tzn. i domácnosti.

Jako první se nabízí skupina firem kolem stále státní společnosti ČEZ ("superČEZ"). Do této skupiny můžeme zařadit firmu Středočeská energetika. SČE se rozhodla využít aplikaci Oracle CRM (implementaci provedla Logica). V roce 2002 byla dokončena implementace CRM řešení Siebel eEnergy od firmy Siebel Systems (hlavní podíl na implementaci - Hewlett-Packard) v distribuční společnosti Severomoravská energetika, což je další firma působící s rámci uskupení "superČEZ" (jde o největší z regionálních distribučních společností v ČR). Západočeská energetika se rozhodla pro CRM řešení využívající technologie SAS a Siebel Systems a tým odborníků spolu s konzultační firmou Soluziona na implementaci začal pracovat rovněž v roce 2002. Čtvrtou firmou z této skupiny je firma Východočeská energetika, která již využívá řešení mySAP.com CRM uvedené do provozu již skoro před třemi lety, v červnu 2002. Poslední firmou je Severočeská energetika, kde ale musí podle rozhodnutí Antimonopolního úřadu ČEZ do září 2004 prodat svůj majoritní podíl, čímž by Severočeská energetika z tohoto uskupení vypadla. Nicméně tato firma využívá řešení firem ORACLE a SAP.

Tabulka 3 – Řešení CRM ve skupině ČEZ

Firma	Řešení CRM
Středočeská energetika	Oracle CRM/ Oracle
Severomoravská energetika	Siebel eEnergy/Siebel Systems
Západočeská energetika	Siebel Systems/SAS
Východočeská energetika	mySAP.com CRM/SAP
Severočeská energetika	Oracle a SAP

Jelikož došlo k utvoření "superČEZu" před jednotlivými rozhodnutími o výběru dodavatelů CRM řešení, bude se zřejmě s největší pravděpodobností muset dodatečně rozhodnout o jednotné platformě, na které bude skupina do budoucna pracovat. Tento krok je naprosto nevyhnutelný nejen z hlediska budoucího fungování jednotlivých systémů a možnosti jejich propojení, ale i s ohledem na jejich servis, správu, up-date a up-grade a náklady s tímto spojenými. Nehledě už na problémy při migraci pracovní síly uvnitř skupiny. Toto rozhodnutí se musí udělat i s ohledem na plánované akvizice v zahraničí, o které firma ČEZ v současné době usiluje (Polsko, Slovensko, Bulharsko).

Druhou velkou energetickou skupinou (největší soukromou energetickou firmou na světě a největší v Evropě) v ČR je "skupina E.ON". Tato skupina obsahuje především dvě regionální distribuční firmy a tj. Jihočeská a Jihomoravská energetika a dále pak tři podíly v distribucích plynu (Západočeská plynárenská, Jihomoravská plynárenská a Jihočeská plynárenská). Obě firmy věnující se distribuci elektrické energie používají odvětvové CRM řešení mySAP.com/Utility. E.ON navíc otevřeně deklaroval rozhodnutí o celosvětovém používání SAP řešení u všech svých dceřinných firem, včetně České republiky.

Tabulka 4 – Řešení CRM ve skupině E.ON

Firma	Řešení CRM
Jihočeská energetika	mySAP.com/Utility
Jihomoravská energetika	

Hlavně plynárenskou skupinou v ČR je "RWE skupina", vlastníci většinou majoritní podíly v českých distribucích plynu. Všechny regionální distribuční společnosti plynu (kromě Pražské plynárenské) a Transgas, opět globálně využívají SAP řešení.

Další skupinou je tzv. "Pražský holding", který sice není majetkově propojen v jednu firmu, ale významným vlastníkem je město Praha, mající tomu odpovídající rozhodovací slovo. Tyto firmy by mohly vzhledem ke svému počtu zákazníků na územní hlavního města Praha úspěšně využívat synergických efektů, v případě společné fakturace všech odebraných služeb a produktů (plyn, elektřina, voda), servisu, komunikace se zákazníky atd. Což by samozřejmě v tržním prostředí představovalo nutnost rozsáhlého propojení ERP systému, což částečně představuje CRM i billingové řešení. Pražské energetika nevyužívá plnohodnotné CRM, ale zákaznický servis probíhá již od roku 2001 přes řešení NESS CEE/ORACLE/SAP. Pražské plynárny vsadily na PVODwinŽCRM a Pražské vodovody a kanalizace na LCS Noris/CRM.

Poslední velkou, ovšem pouze potencionální skupinou zákazníků pro CRM řešení v energetickém průmyslu jsou začínající licencovaní obchodníci s elektrickou energií (na základě energetického zákona), firmy věnující se obchodu se energetickými surovinami apod., kteří zřejmě budou potřebovat CRM systémy, pro řešení jejich zákaznických vztahů. Jako příklad uveďme firmu Tchas z Ostravy. Ta se rozhodla implementovat řešení Oracle CRM.

8 Problematika praktického využití dvou typů portálů

8.1 Služby velkoodběratelům na internetu (JČE)

Zákaznický portál Jihočeské energetiky byl funkční od roku 2001 do roku 2004. Byl přístupný pouze pro významné zákazníky – velkoodběratele, kteří projevíli zájem o tuto službu. Nabízel aktuální přehled o jejich současných energetických nárocích a umožňoval i nahlížet do historie odběrů, vše dělené dle jednotlivých odběrných míst či plátce.

Aplikace však měla i další funkce. Umožňovala zobrazené sestavy tisknout a ukládat do zpracovatelného tvaru. Zpracovatelného znamená, že uloženou tabulku bylo možné si otevřít například v programu Microsoft Excel a na tyto data pak aplikovat Vámi specifikované vzorce. Dále systém ze souborů dat generoval grafy a umožňoval tak sledovat výsledky ve zjednodušené podobě. Další funkcí byla optimalizace sazby, pomocí které si zákazník mohl vypočítat správnou sazbu pro svůj odběr na následující období. K dispozici bylo i nastavení vzhledu, kde jste si mohli libovolně vybrat z předpřipravených schémat barev tabulek či úvodní graf, který se zobrazoval vždy na úvodní stránce.

Tento portál byl vůbec jeden z prvních zákaznických portálů energetické firmy v ČR a zaznamenal ve své době velikou úspěšnost.

8.1.1 Technický popis

S ohledem na bezpečnost životně důležitých dat firmy nebyl portál nepojen online na interní zákaznický systém (ZIS). Data byla nejprve zpracována v systému SAP a poté přenesena ve fakturačních cyklech na portál. Zde je důležité poznamenat, že toto řešení mělo nejen významný bezpečnostní charakter, ale také podstatný vliv na rychlost celé aplikace. Na portál totiž nebyla zbytečně přenášena data všech zákazníků, ale pouze těch kteří si o ně zažádali u svého obchodníka s elektřinou.

Přístup na portál byl možný po zadání čísla odběrného místa a hesla, které si zákazník mohl sám zvolit. Tato autentizace byla v té době dostatečná, neboť portál neumožňoval jakékoliv změny v datech přihlášeného zákazníka.

Samotný portál byl technicky řešen jako oddělená aplikace napsaná v programovacím jazyku PHP a nainstalovaná v privátní části veřejného web serveru Jihočeské energetiky. Web server Apache byl umístěn v demilitarizované zóně firewallu

a v nastavených intervalech (zpravidla v noci, kdy nezatěžoval samotné CRM systémy) si stahoval připravené dávkové soubory s daty zákazníků z interních systémů.

K bezproblémovému fungování portálu postačoval zákazníkovi pouze Microsoft Internet Explorer verze 4.0 a vyšší nebo Netscape Navigátor verze 4.0 a vyšší.

8.1.2 Přehled funkcí

8.1.2.1 Přihlášení

Po zadání správné web adresy se zobrazila přihlašovací stránka portálu (obr. 8.1). Zde bylo třeba vyplnit korektní identifikační údaje získané dříve od obchodníka s elektřinou.

21. únor, 2001 Kdo jsme | Pro zákazníky | Pro investory | Pro obchodní partnery | Pro veřejnost

Služby velkoodběratelům na Internetu

Obchodní podmínky | Ceník elektřiny | Přehled sazeb | Fakturace a platby | Kontakty Help

Osobní stránky zákazníků

Identifikace: 123456789

Heslo:

Plátce ☐ Odběrné místo ☐

Přihlášení Reset

Na následujících stránkách mohou zákazníci Jihočeské energetiky najít historické údaje o odběru ve svém odběrném místě. Přístup k údajům získáte po přihlášení do systému.

Kdo jsme | Pro zákazníky | Pro investory | Pro obchodní partnery | Pro veřejnost

©2000 Jihočeská energetika, a.s.

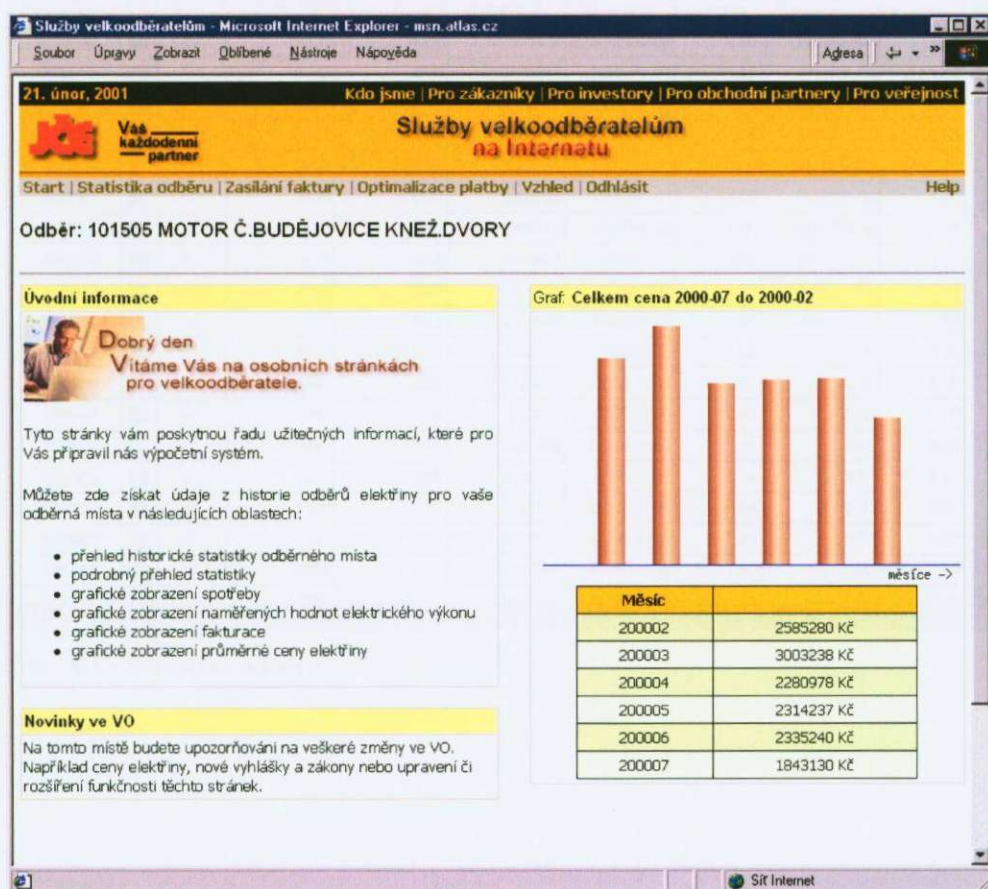
Obr. 8.1 - Přihlášení

8.1.2.2 Homepage portálu

Pokud autentizace proběhla úspěšně, zákazník se dostal na svou homepage vlastního portálu (obr. 8.2) kde v horní části obrazovky viděl název a číslo svého odběrného místa.

V pravé části je zobrazen graf a tabulka vývoje jeho plateb za elektřinu za posledních 6 měsíců. Kliknutím na graf se dostanete do sekce, kde si můžete prohlédnout v grafickém znázornění další zajímavé údaje (podrobněji viz. bod 8.1.2.5 tohoto návodu). Typ grafu zobrazeného na úvodní obrazovce lze zvolit.

Vzhled úvodní obrazovky si lze dále přizpůsobit po kliknutí na položku *Vzhled* v horním menu. Zároveň zde můžete zapnout funkci *Novinky*, která znamená to, že po přihlášení se Vám bude na první stránce zobrazovat okno s aktuálními novinkami pro velkoodběratele.



Obr. 8.2 - Úvodní stránka

8.1.2.3 Statistika odběru

Na této stránce jsou zobrazeny celkové historické údaje odběrného místa seřazené po měsících od aktuálního data za cca poslední 3 roky.

Kliknutí v levém sloupci na konkrétní měsíc zobrazíte přehled kompletních odběrových statistik hledaného období (datum je zobrazen ve formátu "rokměsíc").

V detailním pohledu na vybrané období se můžete posunovat o 1 nebo 12 měsíců vpřed či vzad a po kliknutí na ikonu grafu u zvoleného období se dostanete na grafické znázornění odběrů (viz bod 8.1.2.5.).

Služby velkoodběratelům - Microsoft Internet Explorer - msn.atlas.cz

Soubor Úpravy Zobrazení Oblíbené Nástroje Nápověda Agresa

21. únor, 2001 Kdo jsme | Pro zákazníky | Pro investory | Pro obchodní partnery | Pro veřejnost

Služby velkoodběratelům na Internetu

Start | Statistika odběru | Zaslání faktury | Optimalizace platby | Vzhled | Odhlásit Help

Odběr: 101505 MOTOR Č.BUDĚJOVICE KNEŽDVOŘY

Fa. odběr	Sazba	Sjedn. kW	Naměř. kW	Spotř. kWh	Kč celkem	Kč/kWh	Kč bez DPH	Kč/kWh
200007	B1c	3400	3366	971122	1843130.00	1.90	1510813.00	1.56
200006	B1c	3400	3370	1439212	2335240.00	1.62	1914196.00	1.33
200005	B1c	3400	3363	1420344	2314237.00	1.63	1896980.00	1.34
200004	B1c	3400	3381	1388521	2280978.00	1.64	1869717.00	1.35
200003	B1c	3400	3366	1513439	3003238.00	1.98	2461754.00	1.63
200002	B1c	3400	3373	1205065	2585280.00	2.15	2119154.00	1.76
200001	B1c	3400	3366	1309146	2697046.00	2.06	2210769.00	1.69
199912	B1	3400	3359	1175877	2306452.00	1.96	1890599.00	1.61
199911	B1	3400	3362	1524331	2634050.00	1.73	2159130.00	1.42
199910	B1	3400	3311	1260980	2386473.00	1.89	1956192.00	1.55
199909	B1	3400	3319	1203727	2309803.00	1.92	0.00	0.00
199908	B1	3540	3535	1128082	2275514.00	2.02	0.00	0.00
199907	B1	3360	3234	772524	1902747.00	2.46	0.00	0.00
199906	B1	3360	3340	1327982	2410160.00	1.81	0.00	0.00
199905	B1	3360	3256	1141317	2239692.00	1.96	0.00	0.00
199904	B1	3360	3219	1288967	2373415.00	1.84	0.00	0.00
199903	B1	3360	3337	1477800	2574431.00	1.74	0.00	0.00
199902	B1	3360	3274	1157365	2275231.00	1.97	0.00	0.00
199901	B1	3400	3364	1330311	2443350.00	1.84	0.00	0.00

SIX Internet

Obr. 8.3 - Statistika odběru

Služby velkoobchodům - Microsoft Internet Explorer - msa.dlas.cz

Soubor Úpravy Zobrazení Oblíbené Náhled Nápověda Adresa

21. únor, 2001 Kdo jsme | Pro zákazníky | Pro inventory | Pro obchodní partnery | Pro veřejnost

Služby velkoobchodatelům na internetu

Start | Statistika odběru | Zaslání faktury | Optimalizace platby | Vzhled | Odhlásit Help

Odběr:

od 1999-06 do 2000-06

-12 -1 Měsíc +1 +12

Období	Sazba	Špička kWh	Vysoká kWh	Nízká kWh	Celkem kWh	Tech. max kW	Naměř. max kW	Sjed. max Kč	Účtov. max	Nedoř. max	Překr. sjed. kWh	Sjed. VD kWh	Poskyt. VD
199906	B1	225625	609223	413134	1327982	4000	3340	3360	3360	20			
199907	B1	130502	410091	231931	772524	4000	3234	3360	3360	126			
199908	B1	203539	620216	304327	1128082	4000	3535	3540	3540	5			
199909	B1	206753	657324	339650	1203727	4000	3319	3400	3400	81			
199910	B1	327169	565687	368104	1260980	4000	3311	3400	3400	89			
199911	B1	404900	660903	458528	1524331	4000	3362	3400	3400	38			
199912	B1	313042	500879	361956	1175877	4000	3399	3400	3400	41			
200001	B1c	353045	506534	449567	1309146	4000	3366	3400	3400	34			
200002	B1c	343836	532547	329682	1205065	4000	3373	3400	3400	27			
200003	B1c	418704	610257	494478	1513439	4000	3366	3400	3400	34			
200004	B1c	224545	730587	433389	1388521	4000	3381	3400	3400	19			
200005	B1c	220300	749796	442240	1420344	4000	3363	3400	3400	37			
Celkem		3379903	7234044	4615906	15230010	40000	40309	40060	40060	514			

Období	Sazba	Špička Kč	Vysoká Kč	Nízká Kč	Celkem Kč	Tech. max Kč	Naměř. max Kč	Sjed. max Kč	Překr. sjed. Kč
199906	B1	257212,5	627192,93	330507	1214911	441600			753640

Holovo Sit Internet

Obr. 8.4 - Statistika odběru - pohled na zvolené období

8.1.2.4 Detailní statistika odběru

Na této stránce jsou zobrazeny detailní údaje odběrného místa seřazené po měsíci. Výpis pro porovnání obsahuje údaje za 12 měsíců.

Pro přechod na jiné období slouží červená tlačítka nad tabulkou. Těmito tlačítky můžete ovládat přesun o 1, resp. 6 měsíců vpřed, nebo vzad. Po kliknutí na vybrané tlačítko se Vám zobrazí odpovídající časové období s novými údaji.

Ve spodní části stránky (pod tabulkou) najdete odkaz pro vytisknutí nebo uložení stránky. Po kliknutí se stránka

99712	B1	3300	3223	883634	1730430,0
99711	B1	3300	3219	1272416	2041315,0
99710	B1	3300	3226	1349567	2104730,0
99709	B1	3300	3201	1156086	1925034,0
99700	B1	3300	3215	1120424	1899414,0

Tisk a uložení

Kdo jsme | Pro zákazníky | Pro inventory | Pro obchodní partnery

zkonvertuje na formát vhodný pro tisk. Zde můžete zvolit buď uložení nebo tisk. Jestliže zvolíte uložení, otevře se Vám standardní dialogové okno pro uložení souboru. Tento soubor je exportován ve formátu *.csv, který můžete přečíst např. pomocí programu MS Excel. Jestliže zvolíte tisk, otevře se standardní dialogové okno s dotazem před tiskem.

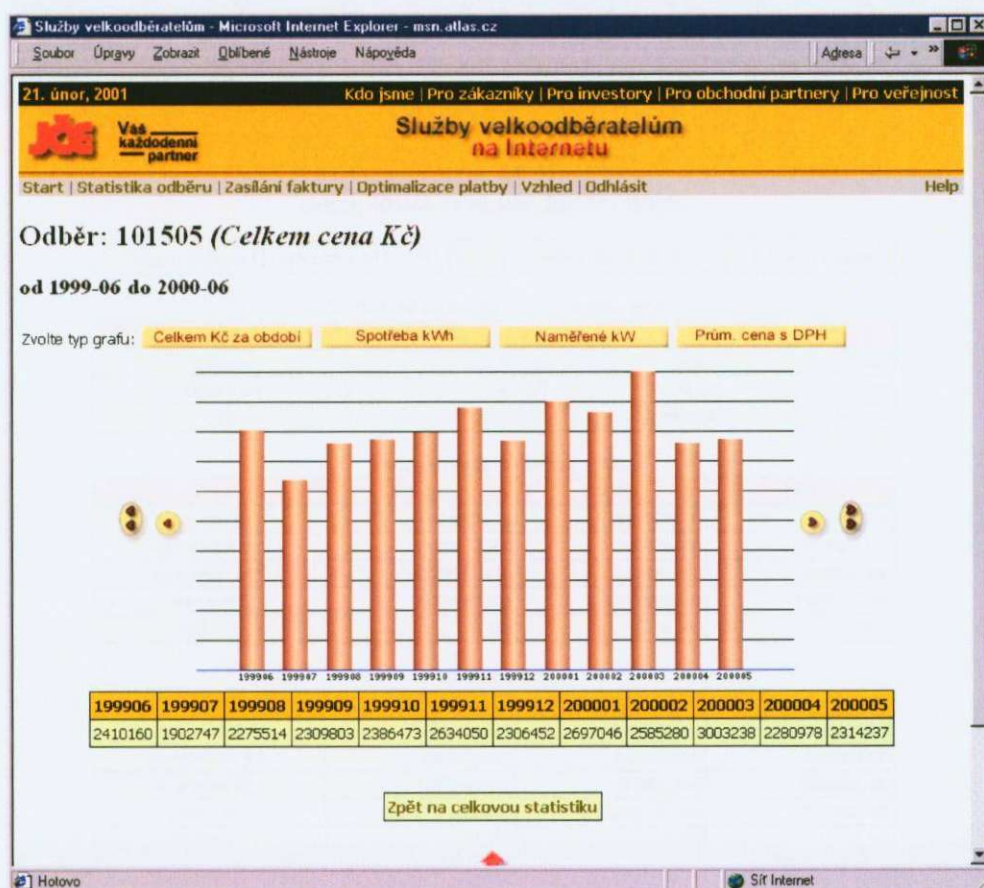
Obr. 8.4 - Statistika odběru – export, uložení a tisk dat

8.1.2.5 Grafické zobrazení

Na této stránce si můžete zobrazit Vaše odběrové statistiky ve sloupcových grafech. Je zde zobrazen graf pro vybrané období plus tabulka hodnot. Časové období můžete posouvat pomocí šipek umístěných po stranách grafu. Jednoduchá šipka znamená posun vřed, či vzad o jeden měsíc. Dvojitá šipka umožňuje posun o 12 měsíců.

K výběru jsou tyto typy grafů:

- Celkem Kč za období
- Spotřeba kWh
- Naměřené kW
- Průměrná cena s DPH



Obr. 8.5 - Grafické zobrazení

8.1.2.6 Stanovení optimální sazby

Tato funkce slouží ke nalezení optimální sazby. Data, pomocí kterých bude vypočten odhad, jsou získávána z historických údajů konkrétního odběrného místa.

Ceník, podle kterého se sazby počítají, je zobrazen v horní části tabulky.

První tabulka zobrazuje technické hodnoty, které jsou použity k výpočtům. Další tabulka zobrazuje vypočtené hodnoty v korunách. Program Vám ve třetí tabulce doporučí, jaká sazba by mohla být pro Váš odběr nejvýhodnější.

Stisknutím tlačítka *Vložení vlastních KWh* se dostáváte do části určené pro vlastní modifikaci dat. Můžete si vybrat období vstupních dat, které chcete upravovat a současně nastavit sazbu pro výpočet. V tabulce můžete upravit libovolný údaj a po stisknutí tlačítka *Dopočítat* získáte doporučení pro výběr sazby. Pro porovnání Vám program nabízí výstup i v ostatních sazbách.

Samozřejmě i zde máte možnost stránku vytisknout či uložit po kliknutí na symbol diskety a tiskárny ve spodní části stránky.

Služby velkoodběratelům - Microsoft Internet Explorer - msn.atlas.cz

Soubor Úpravy Zobrazit Oblíbené Nástroje Nápověda | Agresa

21. února, 2001 Kdo jsme | Pro zákazníky | Pro investory | Pro obchodní partnery | Pro veřejnost

Váš každodenní partner **Služby velkoodběratelům na internetu**

Start | Statistika odběru | Zaslání faktury | Optimalizace platby | Vzhled | Odhlásit Help

Odběr: 101505 za období: 200007 - 199908

Vyberte si z ceníků:

Technické hodnoty součty sazba B1c

	Celkem	Léto	Zima
Tech. max	48000	24000	24000
Účtované kW	40940	20540	20400
kWh	15539846	7551008	7988838

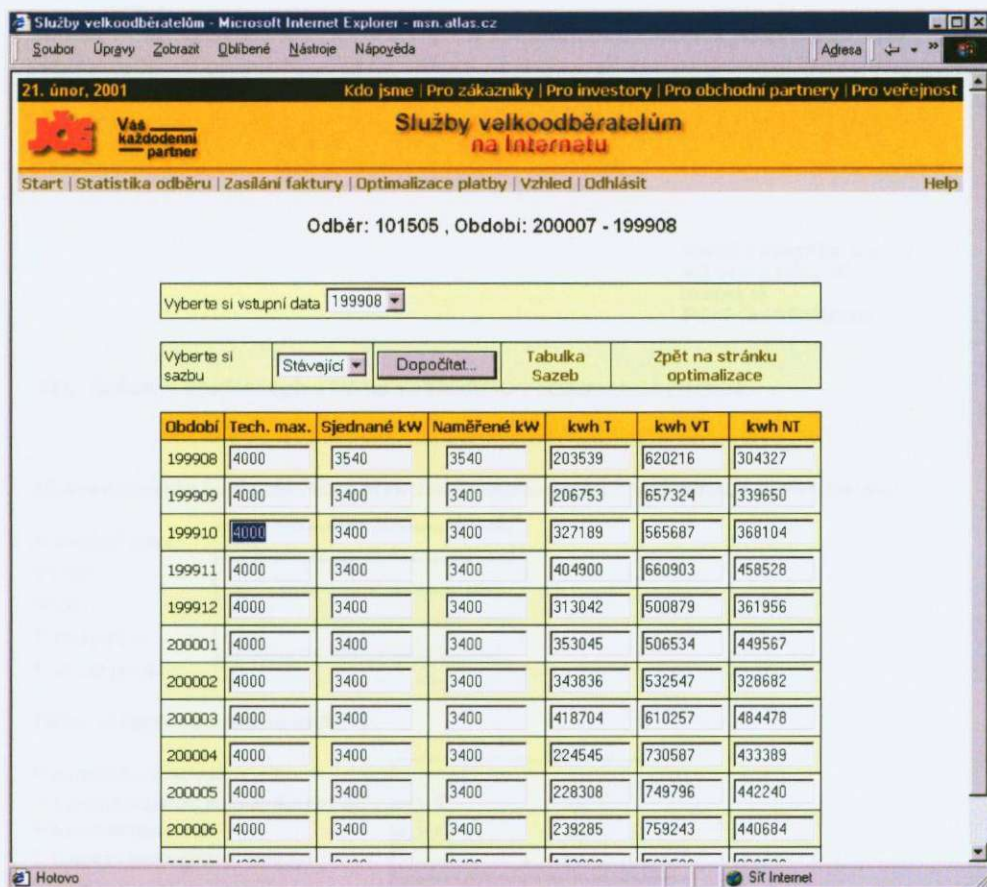
Současná (B1c) sazba v Kč

	Celkem	Léto	Zima
Tech. max (Kč)	3696000.000	1848000.000	1848000.000
Účtované kW (Kč)	6302170.000	2783170.000	3519000.000
El. energie (Kč)	17275483.820	7376961.640	9898522.180
Celkem (Kč)	27273653.820	12008131.640	15265522.180
Kč/kWh	1.755	1.590	1.911

Doporučení B1c

	Celkem	Léto	Zima
Tech. max (Kč)	3696000.000	1848000.000	1848000.000
Účtované kW (Kč)	6302170.000	2783170.000	3519000.000
El. energie (Kč)	17275483.820	7376961.640	9898522.180
Celkem (Kč)	27273653.820	12008131.640	15265522.180
Kč/kWh	1.755	1.590	1.911

Obr. 8.6 - Výpočet optimální sazby



Obr. 8.7 - Výpočet optimální sazby - vložení vlastních dat

8.1.2.7 Zaslání faktury

Zde portál nabízel prostřednictvím internetu pravidelné zasílání opisu faktur za elektřinu a u registračních měření zátěžových profilů i naměřené hodnoty 1/4 hod. maxim, tzv. archivů. Fakturační údaje tak zákazník získal prakticky ihned po jejich vyhotovení a měl je k dispozici o několik dní dříve, než klasickou poštovní zásilkou.

Tato služba se objednávala tak, že zákazník nejprve vyplnil a vytiskl žádost o zaslání opisu faktur za elektřinu v elektronické podobě. Poté bylo nutné, kvůli nedořešené legislativní problematice elektronického podpisu, žádost ručně podepsat a odeslat „klasickou poštou“ na adresu Jihočeské energetiky, a.s.

Žádost o zaslání opisu faktur - Microsoft Internet Explorer - man.atlas.cz

Soubor Úpravy Zobrazení Oblíbené Nástroje nápověda Adresa

JČE

Jihočeská energetika, a. s.
odd. péče o klienty VO
Lánovská 16
370 49 České Budějovice

Věc: Žádost o zaslání opisu faktur za elektřinu v elektronické podobě

Žádáme o pravidelné zaslání opisu faktur za elektřinu vystavených Jihočeskou energetikou, a. s. pro odběratele:

► obchodní jméno:

► sídlo:

► IČO:

► číslo platezce:

► adresa platezce:

Faktury za elektřinu požadujeme zasílat:

► na e-mailovou adresu:

► s archivem 1/4hod. naměřených hodnot: ANO ☐ NE ☐

► s kryptováním údajů: ANO ☐ NE ☐

► kontaktní osoba (jméno, funkce):

► telefon, e-mail:

Hotovo

SiX Internet

Obr. 8.8 - Žádost o zaslání opisu faktur

8.1.2.8 Help

V případě nejasností v ovládání aplikace byla samozřejmě k dispozici kontextová nápověda, kterou šlo kdykoliv otevřít kliknutím na tlačítko *Help* v pravém horním rohu zobrazené stránky, popř. zaslat informační email či zavolat na Hot-Line.

8.2 Portál pro velkoodběratele (E.ON)

Zákaznický portál E.ONu je v současné době ve stádiu dokončování a pro zákazníky bude přístupný v prvním čtvrtletí roku 2006. Díky sloučení Jihočeské energetiky (JČE) a Jihomoravské energetiky (JME) do jediné společnosti – E.ON - bude i jeden portál společný pro odběratele obou těchto již bývalých firem.

The screenshot displays the SAP Enterprise Portal 6.0 interface in a Microsoft Internet Explorer browser window. The page title is "Zobrazení informací o místě spotřeby" (Display information about the consumption location). The left sidebar contains navigation links: Úvod, Zákazník, Místo spotřeby, Historie spotřeby, Přehled plateb, E.ON kontakt, and Průběhové měření. The main content area shows a search for "Místo spotřeby: 3101037716". Below this, there are two tables. The first table, "Informace o místě spotřeby", lists basic data, meter information, and location details. The second table, "Kontaktní osoba zákazníka pro místo spotřeby", lists contact information for the location.

Informace o místě spotřeby	
Základní údaje	
Místo spotřeby	3101037716
Odběrné místo - obchodní	4101040859
Odběrné místo - distribuční	4101040655
Volitelný název místa spotřeby	
Popis místa spotřeby	Kaufland Česká republika v.o.s supermarket
Ulice, č.p./č.o.	Kamenice /1260
Obec	Brno
PSČ	625 00
Obchodník s elektřinou	E.ON ENERGIE, A.S.
Distributor elektřiny	E.ON ENERGIE, A.S.
Číslo smlouvy	
Odebíraný produkt	VO-OB smluvní neodešel SD (08)
Modifikace produktu	ExtraPower
Napětová hladina	22 kV (VN)
Způsob odečtu	PRŮBĚHOVÉ MĚŘENÍ TYPU B (RUČNÍ ODEČET)
Spolehlivost dodávky	standardní

Kontaktní osoba zákazníka pro místo spotřeby (zavedení kontaktu)	
Příjmení	
Jméno	
Titul	
Telefon	241 051 221
Fax	241 717 260
E-mail	mailmaster@kaufland-online
Ulice	Pod víšňovkou
Číslo poštovní	1661

Obr. 8.9 - Portál E.ON - Zobrazení informací o místě spotřeby

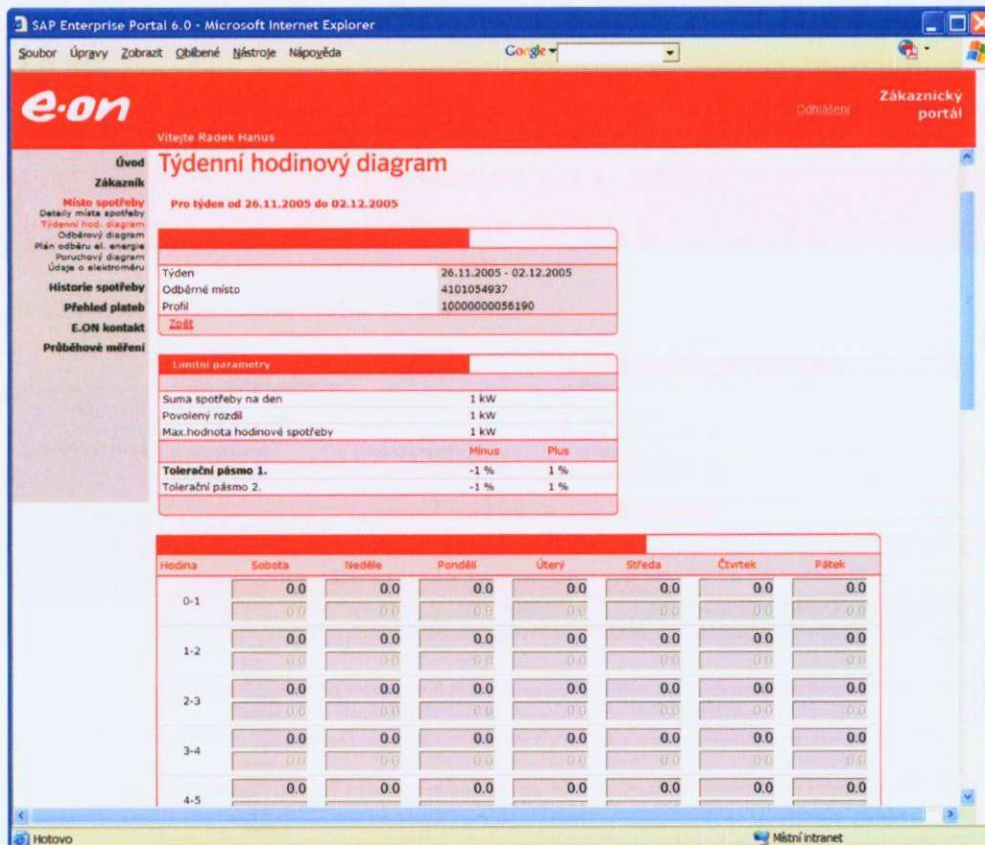
Protože E.ON veřejně deklaroval celopodnikové podporování SAP systémů, je portál vyvíjen kompletně na SAP technologii. Koncovým bodem je SAP Enterprise Portal (dále SAP EP) verze 6.0, který lze použít jako portál externí i interní.

Několik vlastností SAP EP:

- Nezávislost na použité platformě
- Založený na web přístupu, uživatelských rolích a autentizaci
- Centralizovaný přístup ke všem SAP i nonSAP systémům
- Integrace a strukturalizace všech typů informací
- Vystavěn na otevřených standardech
- Propracované možnosti navigace

8.2.1 Technický popis

Portál E.Onu je opět internetové řešení komunikace se zákazníky resp. s partnery. Slouží k zobrazování údajů z vnitřního informačního (zákaznického) systému (ZIS) a rovněž umožňuje provádět operace a změny, jejichž výsledkem jsou smluvní úkony např. změna sazby, ukončení odběru, úprava odběrového diagramu apod.



Obr. 8.10 - Týdenní hodinový diagram

O portálu se v této souvislosti uvažuje samozřejmě jako o bezplatné službě zákazníkům a partnerům. Vzhledem k povaze úkonů prováděných na portálu, je nezbytné dbát na bezpečnostní hledisko celého řešení. Na druhou stranu však zvolené řešení přístupu na portál musí být akceptovatelné zákazníkem z pohledu uživatelské přívětivosti a praktického využití. Pro oblast prodeje velkoodběratelům (VO) a Distribuce bylo navrženo řešení využívající softwarový certifikát. Pro prodej domácnostem (MOO) a menším podnikatelům (MOP) je doporučeno jednodušší řešení, které je snadnější pro používání běžným uživatelem.

Protože tento portál obsahuje již velmi mnoho funkcí, bylo by velmi zdlouhavé je zde jednotlivě popisovat. Navíc je stále ve vývoji, takže se některé funkčnosti mohou ještě změnit. Připojil jsem proto pouze seznam implementovaných scénářů a několik

obrazovek, které obsahuje tato kapitola. Seznam scénářů VO implementovaných v portálu obsahuje tabulka 5.

Scénářem se rozumí zpravidla hlavní obrazovka jedné úlohy, která může obsahovat další vložené podstránky, případně významná funkcionalita portálu.

V tomto řešení je použito standardní řešení SAP. Data jsou získávána ze SAP IS-U a SAP CRM systémů. Jako webový server je použit server na bázi SAP WAS + portál SAP EP.

SAP Enterprise Portal 6.0 - Microsoft Internet Explorer

Soubor Úpravy Zobrazit Ověřit Nástroje Nápověda

e-on Vítejte Radek Hanus Zákaznický portal

Úvod
Zákazník
 Místo spotřeby
 Detaily místa spotřeby
 Týdenní hod. diagram
 Odběrný diagram
Plán odběru el. energie
 Poruchový diagram
 Údaje o elektroně
Historie spotřeby
 Přehled plateb
 E.ON kontakt
 Průběhové měření

Plán odběru elektrické energie

Místo spotřeby: 3101037716 Rok: 2005

Zákazník	Dodavatel
Kaufland Česká republika v.o.s. Pod višňovkou 25 /25 Praha 4 140 00 IČ (RČ): 25110161 DIČ: CZ25110161	E.ON Energie, a.s. Lannova 205/16 České Budějovice 370 49 IČ (RČ): 26078201 DIČ: CZ26078201

Adresa místa spotřeby (odběrného místa)
Kamerice 1260, Brno 625 00

Čtvrtletí	Měsíc	Plánovaná množství elektrické energie Měsíční [kWh]	Čtvrtletní [kWh]	Měsíční rezervovaná kapacita [kW]
1.	Leden Únor Březen			
2.	Duben Květen Červen	30	30	30
3.	Červenec Srpen Září	20	20	20
4.	Říjen Listopad Prosinec			

Regulační skupina na období

Hotovo Místní intranet

Obr. 8.11 - Plán odběru elektrické energie

Pro potřeby autentifikace je použit server s instalovanou službou Apache. Z důvodu bezpečnosti a rychlosti je zvolen princip off-line s periodicitou aktualizace dat 1x denně. Ke zpracování off-line dat dochází na serveru WAS. Pro scénáře, které vyžadují okamžitou interakci s backendovými systémy SAP IS-U a SAP CRM, je využita komunikace on-line.

Tabulka 5 - Seznam implementovaných scénářů VO na portálu

	Popis scénáře
1	Úvod
2	Historie přístupů

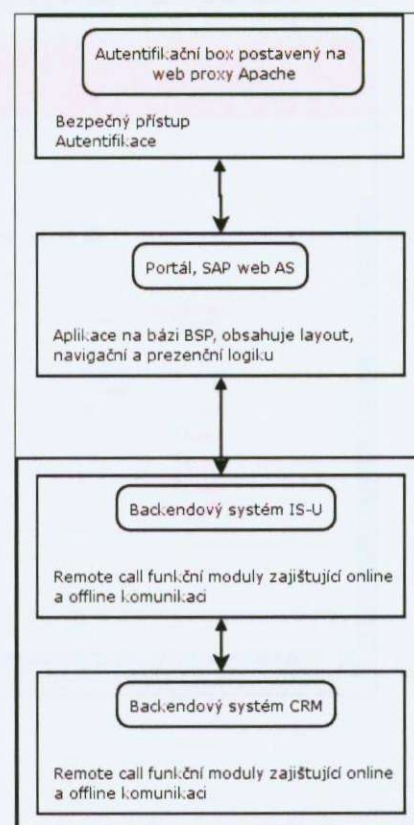
3	Zákazník - detaily
4	Místo spotřeby
5	Detaily místa spotřeby
6	Týdenní hodinový diagram
7	Odběrový diagram
8	Sjednané množství
9	Údaje o elektroměru
10	Historie spotřeby
11	Přehled plateb
12	E.ON Kontakt
13	Formuláře
14	Zobrazení průběhového měření
15	Zobrazení statistiky

8.2.2 Technologické řešení

Uživatel je pro přístup na zákaznický portál ověřen pomocí uživatelského certifikátu. Certifikátem se prokazuje na prezenční vrstvě řešení web serveru Apache, který je nakonfigurován jako web proxy.

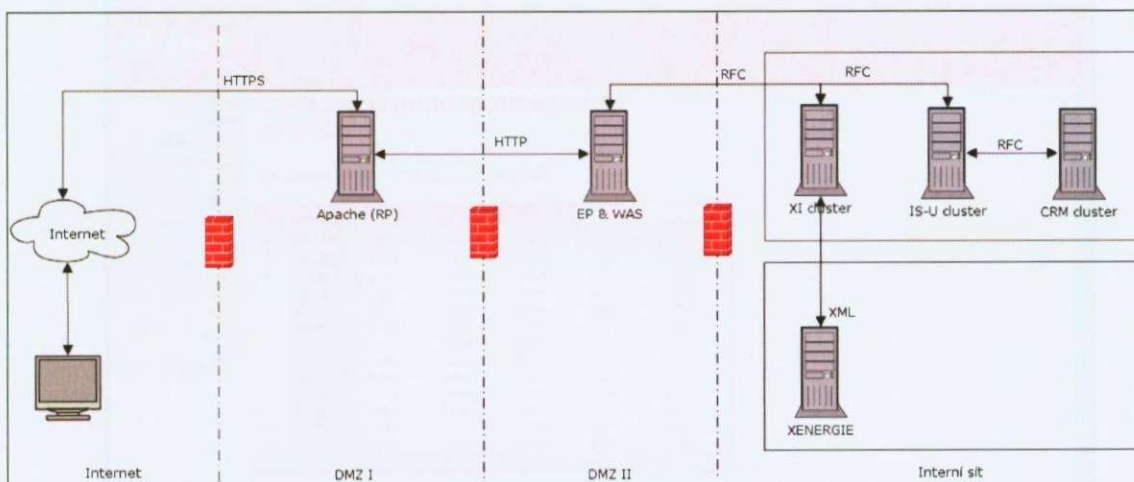
Aplikace SAP BSP (SAP Business Server Pages), obsahuje layout a data zákazníka, který má přístup na portál. Žádná jiná data nejsou na stranu BSP replikována.

Programy a rutiny nutné pro provoz portálu jsou umístěny na systému IS-U, pokud je volán systém CRM tak jedinečně prostřednictvím systému IS-U.



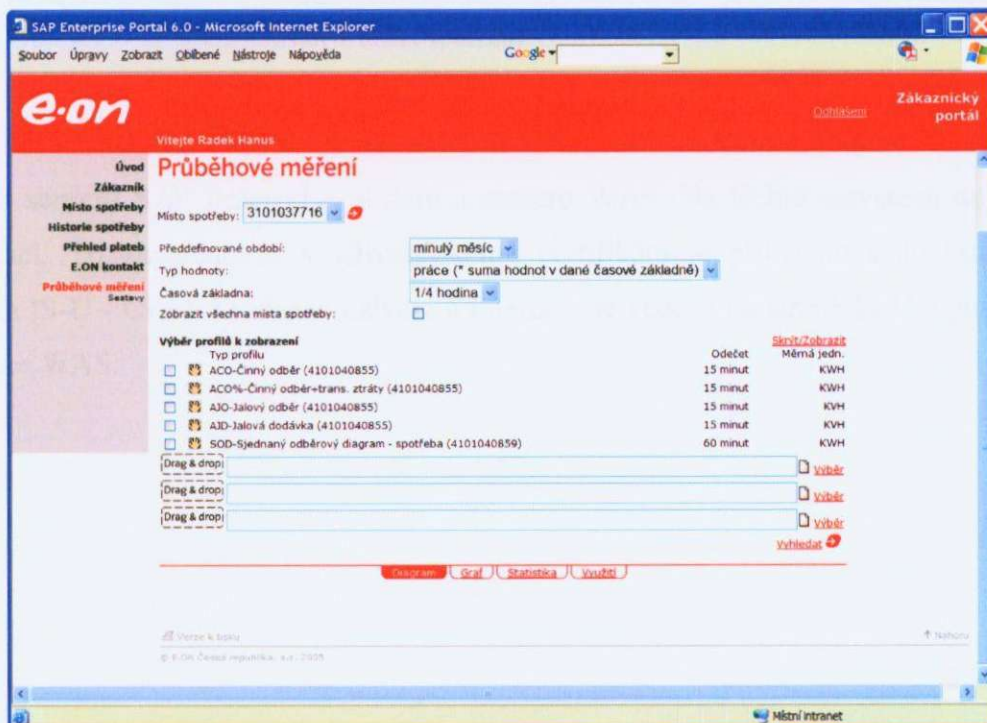
Obr. 8.12 - Technologické řešení

8.2.3 Infrastruktura



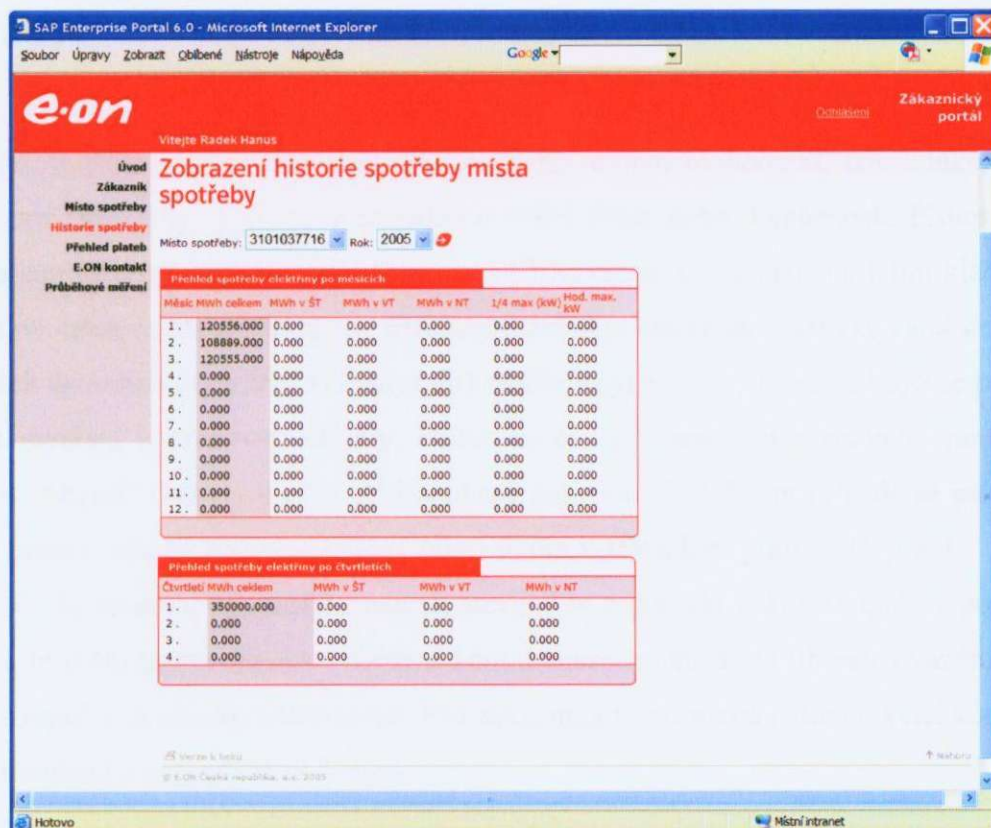
Obr. 8.13 - HW Infrastruktura

Jelikož portál přistupuje přímo online do zákaznického systému, je nutný zvýšený bezpečnostní postup pro přihlášení. Přístup na portál je možný pouze s klientským certifikátem.



Obr. 8.14 - Průběhové měření

Uživatel zákaznického portálu je autentizován uživatelským certifikátem dle standardu X.509. Autentizaci provádí autentizační box postavený na web serveru Apache. Uživatel internetu s tímto serverem může komunikovat pouze pomocí zabezpečeného protokolu HTTPS.



Obr. 8.15 - Zobrazení historie místa spotřeby

Informace obsažené v certifikátu, jehož platnost je ověřena na straně Apache, je posílána serveru SAP Enterprise portálu a serveru WAS. Na těchto serverech dojde k autorizaci. To znamená že k uživatelskému certifikátu je přiřazeno číslo business partnera IS-U - CRM. Evidence uživatelů internetu je vedena na straně IS-U a posílána na server WAS.

9 Závěr

Jakkoli je rozhodnutí o zavedení tržního prostředí do energetického průmyslu potřebné, je třeba ještě vyčkat na přímé důsledky tohoto rozhodnutí, tzn. konkrétních výhod pro zákazníky, a to ať už se jedná o velké firmy nebo domácnosti. Přínos jistě nebude zapříčiněn hromadnou implementací CRM řešení v energetice a jejím kladným vlivem na vztah se zákazníkem, ale především změnou pracovních návyků zaměstnanců (na všech úrovních organizačních struktur) zmiňovaných firem. A právě když se podaří změnit myšlení a pracovní návyky, budou moci zainteresovaní pracovníci používat všechny "chytré" funkce, které CRM aplikace nabízejí. V ideálním případě se pak tato změna projeví tím, že budou vycházet zákazníkům vstříc a lépe plnit jejich přání.

CRM řešení a zákaznické portály nevznikly z popudu zákazníků, ale z popudu firem, a to mělo jediný důvod – udržení konkurenceschopnosti na liberalizovaném trhu a samozřejmě i zvyšování tržeb/zisků. Pro zákazníka to znamená jediné – větší komfort při komunikaci s energetickou firmou.

9.1 Webové služby

Webové služby se zaměřují na zpřístupnění podnikatelských procesů jako služeb, dostupných prostřednictvím internetu. Zpřístupnění funkčnosti aplikace jako služby není novou myšlenkou. Webové služby však představují standardní přístup, který významně snižuje náklady na implementaci a orientuje výzkumné a vývojové aktivity na jednu množinu standardů a technologií. Tvorba standardů webových služeb je řízena W3C (World Wide Web Consortium) a je aktivně podporována všemi hlavními dodavateli IT. Většina dodavatelů softwaru už nabízí nástroje pro vývoj webových služeb, které lze využít pro vytvoření těchto služeb ze stávajících aplikačních komponent, čímž nabízejí cestu pro migraci do tohoto nového prostředí servisně orientovaných aplikací.

Bez ohledu na širokou podporu ze stran dodavatelů IT se v současné době webové služby zatím nevyužívají v širokém měřítku v podnikatelských portálových aplikacích. Podobně jako ostatní technologie využívané v těchto aplikacích i webové služby musejí zajistit podporu základních služeb včetně bezpečnosti, transakcí a tvorby před tím, než bude tato technologie připravena pro využití v e-podnikatelských aplikacích širokého měřítku. Řada zmíněných standardů je stále v procesu vývoje, a tudíž je spolehlivá platforma webových služeb pro podporu komplexních e-podnikatelských aplikací stále ještě vzdálena. S ohledem na rychlý rozvoj v této oblasti

však nelze pochybovat o tom, že tato technická omezení budou dříve či později vyřešena.

Za pozitivní lze považovat skutečnost, že kombinace relativně nízkých vstupních nákladů a širokého přijetí standardů webových služeb povede k tomu, že se tento přístup patrně stane preferovanou volbou pro implementaci podnikatelských portálových aplikací. Významná je i skutečnost, že tvůrci standardů a technologií webových služeb se mohou poučit z neúspěchů dřívějších přístupů a mají možnost řešit problém e-podnikatelské interoperability v kontextu architektury orientované na služby (SOA) - jíž jsou webové služby významným představitelem - a tak se vyhnout některým problémům, které souvisejí s prostředím založenými na dokumentech (či zprávách).

9.2 Porovnání portálů

Porovnal jsem dva zákaznické portály energetické společnosti. Tato firma prochází zásadní organizační změnou, která se zároveň promítá i do změny postojů k zákazníkovi. Oba portály byly vytvořeny zcela na míru dle požadavků, tak aby s využitím ve své době dostupných technických prostředků, nabídly zákazníkovi co nejširší nabídku informací.

Z technologického hlediska jsou zde vidět tři zásadní rozdíly a zároveň i rozvoj ve využití IT technologií.

Tabulka 6 - Porovnání významných změn portálů

Portál JČE	Portál E.ON
Offline přístup do ZISu	Online přístup do ZISu
Data pouze k prohlížení	Data lze prohlížet i měnit
SW platforma: HTML, PHP	SW platforma: SAP, ABAP, BSP

První portál, portál JČE, nebyl připojen online na zákaznický systém. Data zpracovával dávkově další systém, který je poté předával www serveru, kde probíhala vlastní obsluha zákazníka.

Portál byl naprogramován v jazyku PHP a web server pouze zobrazoval předem připravená data z databáze. Další rozvoj, např. s jinou skupinou programátorů by mohl být zdoluhavý, či problematický. Z principu portál umožňoval pouze prohlížení, kontrolu či stažení zákaznických dat.

Nový portál, portál E.ONu, je napojen přímo do zákaznického systému a umožňuje zobrazení opravdu „živých“ dat. Je naprogramován dle standardů SAP pomocí funkčních modulů, které vyhledají požadovaná data přímo v IS-U. Zpracované informace jsou pomocí SAP Enterprise portálu zobrazeny na webu. Tato technologie je využívána po celém světě, díky čemuž má širokou programátorskou základnu a proto zde nehrozí problém „nečitelnosti“ zdrojového kódu aplikace. Zákazník bude moci data nejen prohlížet, ale může i různě údaje měnit, např. upravovat své odběrové diagramy, atd...

Portál pro E.ON by měl být nasazen do produkce pro velkoodběratele na začátku roku 2006. V roce 2007 se předpokládá rozšíření i na segment obyvatelstva. Tato skupina zákazníků má v současné době k dispozici zákaznický portál Synergie.

Zákaznický portál přináší zákazníkovi větší komfort při spravování svého účtu v utilitní společnosti a v budoucnu bude určitě mít, dle úrovně svého komfortu a užitečnosti, velký vliv na rozhodování zákazníka o svém dodavateli ať už elektrické energie, plynu či vody.

10 Literatura

- [1] BASL J.: Podnikové informační systémy – Podnik v informační společnosti, GRADA Publishing, 2002
- [2] DOHNAL J. a POUR J.: Architektury informačních systémů, Ekopress, 1997
- [3] DOHNAL J.: Řízení vztahu se zákazníky – Procesy, pracovníci, technologie, GRADA Publishing, 2002
- [4] FEURLICHT G. a JANDOŠ J.: Elektronické podnikání s využitím webových služeb, Computer World, 2003
- [5] GOEBEL A. a RITTHALER D.: SAP Enterprise Portal, SAP-PRESS, 2004
- [6] HABÁŇ J.: Portálová řešení – co nich (ne) víme, Ebiz, 2004
- [7] HABÁŇ J. a SODOMKA P.: Integrace podnikových aplikací, CVIS, 2005
- [8] HANÁČEK P. a STAUDEK J.: Bezpečnost informačních systémů, Úřad pro státní informační systém, 2000
- [9] KRÁL O.: Využití CRM v energetickém průmyslu, CVIS, 2004
- [10] KRUG S.: Web design – Nenut'te uživatele přemýšlet!, Computer Press, 2003
- [11] MOLNÁR Z.: Efektivnost informačních systémů, GRADA Publishing, 2000
- [12] NOVOTNÝ O., POUR J. a SLÁNSKÝ D.: Business intelligence – Jak využít bohatství ve vašich datech, VŠE, 2003
- [13] POUR J. a kol.: Informační systémy a elektronické podnikání, VŠE, 2003
- [14] POUR J.: Systémová integrace, VŠE, 2003
- [15] POUR J.: Systémová integrace, VŠE, 2004
- [16] POUR J.: Systémová integrace, VŠE, 2005
- [17] ŘEPA V. : Analýza a návrh informačních systémů, Ekopress, 1997
- [18] TOMEK G., VÁVROVÁ V. a VAŠÍČEK J.: Marketing v energetice, GRADA Publishing, 2002
- [19] WESSLING H.: Aktivní vztah k zákazníkům pomocí CRM, GRADA Publishing, 2003
- [20] Zákon č. 458/2000 Sb. (Energetický zákon) platný od 1.1.2001

10.1 Internetové zdroje

www.cez.cz

www.cvis.cz

www.cw.cz

www.ebiz.cz

www.edi.cz

www.eon.cz

www.ietf.org

www.intersystems.cz

www.jce.cz

www.jme.cz

www.lcs.cz

www.microsoft.cz

www.oracle.com

rainbow.vse.cz

www.rwe.cz

www.sap.com

www.sap.cz

www.si.cz

www.softwareag.com

www.systemonline.cz

www.telnet.cz