POŽADAVKY NA INFORMAČNÍ SYSTÉM PLYNOUCÍ Z INTEGRAČNÍCH NÁROKŮ PODNIKOVÉHO PROSTŘEDÍ

Dušan Kajzar

Slezská univerzita v Opavě, Filozoficko - přírodovědecká fakulta, Ústav informatiky,
Bezručovo nám. 13, 746 01 Opava, e-mail: kajzar@c-box.cz

Abstrakt
Účelem článku je upozornit na důležitost požadavků na informační systém, které plynou z integračních nároků podnikového prostředí, tj. z vlastností okolí, ve kterém bude nový IS provozován. V praxi jde mnohdy o požadavky zákazníkem obecně předpokládané, formulované pouze obecně nebo i nevyslovené.

1. Úvod

Důležitou součástí specifikace zadání a vlastního vývoje podnikového informačního systému (IS) je problematika integrace tohoto IS do stávající infrastruktury IS/IT v podniku. Pod pojmem "stávající infrastruktura" zde mám na mysli okolí, do něhož bude nový IS nasazen, tj. okolí, které je tvořeno:

- stávající HW a SW architekturou podnikových IS, tzn. jinými (spolupracujícími a konkurujícími) IS podniku;
- bezpečnostními předpisy podniku, tzn. požadavky na zajištění ochrany dat a požadované dostupnosti daného IS;
- organizací práce dohledu a správy podnikových IS, monitorovacími a administrátorskými nástroji správců IS;
- organizací podpory koncových uživatelů IS.

Následující obrázek schématicky zdůrazňuje skutečnost, že kromě požadavků na funkčnost nového informačního systému musí analytik brát v úvahu i požadavky vyplývající z integračních nároků podnikového prostředí - tj požadavky plynoucí z vlastností okolí, ve kterém nový IS bude provozován.

Obr. 1: Integrace nového IS do podnikového prostředí

Účelem tohoto článku je upozornit na důležitost požadavků plynoucích z integračních nároků podnikového prostředí. V praxi jde mnohdy o požadavky zákazníkem obecně předpokládané, formulované pouze obecně nebo i nevyslovené. Zanedbá-li analytik vývojové firmy problematiku integračních nároků podnikového prostředí, může dojít k problémům v průběhu akceptace IS, v průběhu zavádění daného IS do provozu či až v průběhu samotného provozu, kdy se nedostatky integrovatelnosti nového IS projeví.

2. Charakteristika skupin požadavků

2.1 Požadavky plynoucí z integrace do stávající HW a SW architektury

Nasazení nového IS může být plánováno na dedikovaných HW komponentách, určených pouze pro tento IS; může však být plánováno i na HW komponentách stávajících, které jsou již v podniku rutinně využívány provozními systémy (subsystémy). Právě o tento druhý případ nám nyní půjde.

Pro nový informační systém může být požadováno například:

- ukládání dat na společném diskovém poli, které je již sdíleno jinými IS podniku,
- umístění SW komponent souběžně se SW komponentami jiných IS na tomtéž hardwaru,
- umístění SW komponent do rámce clusterového řešení, ve kterém jsou již integrovány jiné pracující IS,
- umístění některých HW a SW komponent v demilitarizované zóně podnikové počítačové sítě,
- sdílení společného podnikového portálu, autentizačního centra pro přístup k podnikovým IS,
- apod.

Výše naznačené požadavky mohou významným způsobem ovlivnit celkový návrh vyvíjeného IS. Analytik se při své práci neobejde bez podrobného rozboru stávající architektury podnikových IS a rozboru možností sdílení stávajících HW či SW komponent - z hlediska funkčnosti i výkonnosti.

V této podkapitole upozorním stručně na následující tři oblasti analýzy a návrhu IS:

a) Zmapování stávající architektury podnikových IS, které budou s vyvíjeným systémem spolupracovat.

   Jde o vytvoření základního modelu podnikového prostředí a o podrobné zmapování zejména těch subsystémů, které budou tvořit okolí vyvíjeného IS.
   V okolních subsystémech pak věnujeme pozornost tzv. spolupracujícím systémům - tj. systémům, které budou s vyvíjeným IS jakýmkoli způsobem komunikovat.

   Nejde ovšem jen o podchycení uživatelských datových toků mezi podnikovými systémy. Jde také o podchycení toho, že vyvíjený IS bude využívat komunikační infrastrukturu některého ze stávajících podnikových IS - např. infrastrukturu e-mail serverů či replikačních systémů.

   To pak analytika vede k rozborům a predikcím výkonnosti stávajících systémů, které se budou na provozu nového IS nějakým způsobem podílet. Dále to může vést i ke změně klasifikace některých stávajících systémů z hlediska významu pro podnik. Např. přenášel-li doposud e-mail systém pouze korespondenci zaměstnanců, plnil úlohu podpůrného systému. Po nasazení nového IS však bude přenášet důležitá provozní data - z podpůrného systému se takto může stát rázem systém se strategickým významem pro podnik. Tj. jeho výpadek může vážným způsobem narušit výrobní a obchodní aktivity podniku. Se změnou klasifikace podpůrného systému na systém strategický ovšem souvisí další otázky - např. otázka ochrany a požadované dostupnosti systému, otázka organizace systémové podpory provozu daného systému atd.

b) Zmapování stávající architektury podnikových IS, které budou vyvíjenému systému konkurovat.

   Jde o případy, kdy vyvíjený IS bude sdílet některé HW a SW komponenty stávajících systémů. V současné době je v podnicích běžné, že podnikové IS sdílejí velkokapacitní disková pole, výkonné servery (např. v rámci clusterových řešení), ale sdílejí i zálohovací subsystémy s "backup" síťovými segmenty a magnetopáskovými knihovnami. Zde samozřejmě nesmí analytik opomenout rozbory výkonnostních charakteristik stávajících systémů a predikci výkonnostních charakteristik po nasazení vyvíjeného IS do provozu.

c) Prostudování informační strategie podniku a informací o souběžně vyvíjených IS.

   V této oblasti jde o zmapování dalších záměrů v oblasti vývoje a inovace podnikových IS. Analytik by měl brát v úvahu možný vliv připravovaných IS a souběžně vyvíjených IS. To pak může ovlivnit návrh řešení našeho IS (vliv na funkčnost i výkonnost systému v budoucnu).

Z uvedeného je zřejmé, že zavedení nového IS do provozu může vytvořit nová úzká místa v provozu stávajících podnikových systémů. Zavedení nového IS do provozu tedy pro podnik představuje určitá rizika, která je nutno v rámci analýzy a návrhu nového IS eliminovat.

Analytik musí zmapovat problematiku nového IS jako celku, v kontextu celopodnikové architektury. Mimo jiné to znamená zahrnout do analýzy a návrhu celé datové toky, které se nového IS týkají - od místa vzniku dat až po problematiku zálohování dat ve sdílených magnetopáskových knihovnách, archivace dat v podnikových skladech medií a rušení již nepotřebných dat z provozních databází.

2.2 Požadavky plynoucí z bezpečnostních předpisů podniku

Důležitým zdrojem požadavků na vyvíjený IS jsou bezpečnostní předpisy podniku. Analýza takových dokumentů, jako je „bezpečnostní politika IS/IT“ a „bezpečnostní projekt IS/IT“, nám umožní vytvořit si základní představu o možných požadavcích v oblasti ochrany dat a dostupnosti podnikového IS. Výsledky analýzy dokumentů nám pomohou připravit se na konkrétní rozhovory s kompetentními zástupci zákazníka a získat tak další podklady pro přesnou specifikaci požadavků na vyvíjený IS týkajících se bezpečnosti IS.

Může jít o požadavky technického, technologického i organizačního charakteru, např.:

- požadavky na zajištění bezpečnosti a spolehlivosti provozu nového IS na základě specifikace důležitosti IS pro hlavní podnikové procesy,
- požadavky na zajištění bezpečnosti dat nového IS na základě obchodního významu dat pro podnik a citlivosti dat z hlediska vyzrazení (zveřejnění),
- požadavky na pracovní role, ve kterých budou zaměstnanci při práci se systémem vystupovat, přípustné a nepřípustné kombinace pracovních rolí,
- požadavky na přístupová práva koncových uživatelů k systému plynoucí z definovaných pracovních rolí,
- pravidla pro tvorbu uživatelských identifikací (přihlašovacích jmen a hesel) k systému,
- požadavky na dostupnost systému na základě maximální provozně akceptovatelné doby výpadku,
- požadavky na tzv. recovery time - maximální dobu akceptovatelnou pro obnovu systému ze zálohy,

- požadavky na tzv. recovery point - o kolik dní (hodin) zpět je možné se po havárii systému vrátit, tj. jaká nejstarší data je provozně únosné použít k obnově systému,
- povolené komunikační protokoly a povolené komunikační porty v síťovém prostředí,
- požadavky na tvorbu a správu aplikačních a systémových protokolů (logů) se záznamy o procesech probíhajících v systému a akcích koncových uživatelů,
- požadavky na bezpečnost dat uložených v zálohovacích a archivačních systémech,
- požadavky na bezpečnost přenášených dat – šifrování dat.

Požadavky plynoucí z bezpečnostní politiky a návazných předpisů ovlivňují zásadním způsobem návrh systému, jeho HW a SW architekturu, komunikační toky.
Vyvíjený IS přitom musí být schopen využít stávající bezpečnostní infrastrukturu podniku. Zde mám na mysli např. umístění SW komponent do rámce clusterového řešení, ve kterém jsou již integrovány jiné pracující IS, umístění potřebných HW a SW komponent v demilitarizované zóně podnikové počítačové sítě, sdílení společného podnikového portálu jakožto autentizačního centra pro přístup k podnikovým IS, využití společného zálohovacího a archivačního systému apod.

Z hlediska síťové komunikace je nutno pro nově vyvíjený IS přesně definovat potřebné komunikační protokoly, IP adresy a porty. Komunikační infrastrukturu vyvíjeného IS (včetně komunikace s okolím) je vhodné zachytit grafickým modelem.
V podnicích, které mají vyšší požadavky na bezpečnost svých IS, bývá v oblasti síťové komunikace zakázáno vše, co není výslovně povoleno. Vývojová firma tedy nemůže návrh vyvíjeného IS postavit na zcela volné komunikaci mezi dílčími podnikovými sítěmi. Zpracování komunikačního modelu umožňuje analytikovi danou problematiku prodiskutovat s kompetentními zástupci zákazníka (bezpečnostní referent, správce datových komunikací, HW architekt) a ze strany správců podnikových IS požadovanou komunikaci přes aktivní prvky sítě zajistit.
Zvláštní pozornost je přitom potřeba věnovat komponentám, které budou umístěné v demilitarizované zóně resp. budou s komponentami v demilitarizované zóně komunikovat.

Bezpečnostní předpisy podniku také mohou stanovit, že nový IS nesmí být provozně použit bez zpracovaných plánů pro zvládání krizových situací a návazných havarijních scénářů a recovery postupů. Tímto se dostáváme do oblasti technicko-organizační. Potřebné postupy včetně jejich dokumentace musí pak být řešené v rámci projektu vývoje IS, průběžně konzultované s kompetentními zástupci zákazníka a také nakonec zákazníkem akceptované.

Vliv bezpečnostních požadavků na analýzu a návrh nového IS chci zvláště zdůraznit. Zkušenosti z mé praxe ukazují, že požadavky na ochranu a dostupnost podnikových IS analytici vývojových firem často opomíjejí. O to závažnější dopady pak takové opomenutí má, pokud je zjištěno až v etapě zavádění IS do provozu.
Dodatečné zakomponování požadavků bezpečnostní politiky do vyvíjeného IS může být spojeno s dosti hlubokými zásahy do návrhu IS nebo do již implementovaných částí podnikového IS.

2.3 Požadavky plynoucí z potřeb dohledu a správy podnikových IS

Každý podnikový IS musí vydávat dostatečné informace o stavech, ve kterých se nachází. Tím mám na mysli dostatečné informace z hlediska potřeb správců (administrátorů) systému i z hlediska koncových uživatelů systému - provozního úseku podniku.
Tak jako automobil musí mít svoji přístrojovou desku ukazující rychlost, spotřebu paliva, teplotu motoru atd., musí mít svoji „přístrojovou desku“ i podnikový informační systém. Složitost „přístrojové desky“ a množství sledovaných ukazatelů musí být samozřejmě úměrné složitosti podnikového IS a jeho strategickému významu pro podnik (přístrojová deska letadla je jistě mnohem složitější, než přístrojová deska automobilu).

Dalším zdrojem požadavků na vyvíjený IS je tedy nutně prostředí monitorovacích a administrátorských nástrojů používaných v podniku. Do prostředí monitorovacích a administrátorských nástrojů bude vyvíjený IS nakonec zasazen a s těmito nástroji bude muset komunikovat.

Vyvíjený IS musí být schopen s okolními monitorovacími a administrátorskými nástroji komunikovat pomocí stanoveného rozhraní (interface) a musí uvedeným okolním systémům poskytovat věrohodné a aktuální informace. S tímto souvisí následující okruhy požadavků na vyvíjený IS:

a) Ověřování funkčnosti IS jako celku a jednotlivých dílčích procesů podnikového IS.

   Zde nejde jen o včasnou signalizaci procesů havarovaných a neběžících, ale i o ověření funkčnosti procesů, které se sice jeví jako běžící, ve skutečnosti jsou však v nestandardním stavu a požadované činnosti nevykonávají. Jde tedy o to, aby systém byl schopen signalizovat narušení funkčnosti některého ze svých procesů.
   IS by měl obsahovat SW nástroje které budou poskytovat informace o funkčnosti jednotlivých SW a HW komponent, o přístupnosti důležitých klientských stanic, o dobách odezvy systému, o rychlostech přenosů dat mezi zpracovatelskými uzly apod.

   Takovéto nástroje mohou být buď integrální součástí daného IS, resp. nový IS musí být napojitelný na nástroje standardně v podniku používané.

b) Druhy a umístění systémových protokolů (logů), podrobnost a vypovídací schopnost informací v nich obsažených.

   Jde o informace potřebné pro správce podnikových IS. V této oblasti v praxi většinou nebývají problémy, jelikož systémové logy jsou součástí standardních komponent, tj. operačních systémů, databázových systémů, aplikačních serverů apod.

c) Druhy a umístění aplikačních protokolů (logů), podrobnost a vypovídací schopnost informací v nich obsažených.

   Jde o protokoly zachycující činnost v rámci IS jako celku a v jeho částech - aplikacích. Generování informací do těchto logů je tedy záležitostí programového kódu aplikace. Informace mohou obsahovat např.: kdo a kdy s aplikací pracoval, jaké činnosti provedl apod.
   Generování aplikačních logů, jejich kontrola a archivace může být zakotvena v bezpečnostních předpisech podniku.

d) Možnosti pro on-line zobrazení stavu zpracování dat v závislosti na harmonogramu provozní technologie, kterou daný IS realizuje.

   Informace v aplikačních protokolech mají význam nejen pro audit činností (kdo, kdy a co v aplikaci dělal), ale mají i význam pro zobrazení aktuálního stavu zpracování dat. Tj. pro identifikaci, ve kterém místě technologického postupu se proces zpracování nachází. Z takového protokolu (použitím vhodného SW nástroje) může čerpat např. vedoucí provozu. Ten může zjistit, co již bylo provedeno, kde se nachází data zpracovaná určitým pracovištěm apod. V případě havárie systému pak je možno vcelku přesně určit poslední vykonávané činnosti a činnosti, které se již nestačily provést.

   V podstatě se jedná o možnosti trasování systémových a aplikačních protokolů a vyhodnocování informací v nich obsažených. Součástí IS by tedy měly být nástroje pro čtení informací z těchto protokolů, myslím čtení ve vhodném formátu použitím výběrových filtrů.
   Nelze nutit správce či operátora systému, aby neustále pročítal množství informací v množství souborech umístěných na různých počítačích a v různých adresářích. Je potřeba si uvědomit, že správci a operátoři podnikových IS mívají na starosti více podnikových systémů a subsystémů.

   Pokud správci podnikových IS využívají ke kontrole protokolů jednotné nástroje, je nutné výstupy produkované novým IS přizpůsobit tak, aby údaje nového IS byly standardně používanými nástroji čitelné.

Analytik vývojové firmy si musí uvědomit, že jak provozní úsek, který bude s novým IS pracovat, tak i správci systému potřebují v každém okamžiku vědět, v jakém stavu se provozovaný IS nachází. Úsek provozu ze svého pohledu provozní technologie, správci podnikových IS z pohledu správy IS. Informační systém musí potřebné informace poskytnout. Neposkytuje-li podnikový IS dostatečné informace sám o sobě, podobá se v některých svých částech „černé skříňce“ a je velmi obtížné zajišťovat správu jeho provozu.

2.4 Požadavky plynoucí z organizace podpory koncových uživatelů

Z hlediska názvosloví teorie systémů je podnikový IS systémem sociálně-technickým. Při jeho vývoji je tedy nutné brát v úvahu i takové otázky, jako:

- organizace práce všech uživatelů nového IS,
- organizace podpory uživatelů nového IS.

Zaměřím se pouze na druhou z uvedených otázek. Pod pojmem „podpora uživatelů“ zde rozumím organizaci pracovišť, jejichž úkolem je poskytovat pomoc při řešení vzniklých problémů v rámci podnikového IS, zajišťovat distribuci a instalaci nových verzí SW komponent.

Podporu koncových uživatelů můžeme rozdělit do dvou rovin – rovina provozní technologie a rovina technicko-systémová. Do roviny provozní technologie řadím takové problémy, kdy uživatel potřebuje poradit, jak pomocí své aplikace zajistí požadovanou operaci, případně co si má počít, jestliže aplikace operaci provést odmítá (v čem je chyba?). Do roviny technicko-systémové řadím řešení nestandardních či havarijních stavů podnikového IS, zajišťování distribucí a instalací nových verzí SW komponent, oznamování problémů a koordinaci prací při plánovaných i neplánovaných výpadcích.

Organizace podpory koncových uživatelů nemusí být zdaleka triviální záležitostí, uvědomíme-li si, že existují podniky a podnikové IS s centrálními servery, distribuovanými regionálními subsystémy a řádově tisíci pobočkami na nichž pracují aplikace koncových klientů.

Samozřejmě je výhodou, pokud je v podniku již vybudován funkční systém podpory koncových uživatelů (pro stávající podnikové IS) a můžeme jej pro nově vyvíjený IS také využít.
Pokud tomu tak je, je nutné v rámci projektu vývoje nového IS zpracovat organizační postupy podpory koncových uživatelů a navrhnout jejich integraci do stávající organizační struktury (včetně rozboru dopadů na pracovní vytížení pracovníků podpory apod.).
Pokud tomu tak není, je samozřejmě nutné do požadavků na nově vyvíjený IS zahrnout i vybudování adekvátního systému podpory koncových uživatelů.

Opomene-li analytik otázku organizace podpory koncových uživatelů, může se daný IS zhroutit při prvních rutinních problémech či požadavcích na upgrade. Nemusí být totiž v silách stávajícího útvaru IT podniku problém či vzniklý úkol organizačně zvládnout a jeho řešení řídit.
Naopak - dobře organizovaná podpora koncových uživatelů může v případě problémů podpořit dočasný nouzový provoz systému, spolupracovat s experty IT či s dodavatelem na odstranění problému a tím minimalizovat negativní dopady problému na podnik.

3. Závěr

Účelem článku bylo upozornit na problematiku požadavků na vyvíjený podnikový IS vyplývajících z potřeby budoucí integrace tohoto IS do stávající infrastruktury podnikových IS. Jde většinou o požadavky netýkající se přímo funkčnosti vyvíjeného IS ve smyslu realizace podnikových procesů. Právě proto je zde jisté nebezpečí opomenutí či podcenění popisovaných oblastí.

Opomenutí požadavků plynoucích z integračních nároků podnikového prostředí ze strany vývojové firmy může vážně ohrozit úspěch celého projektu vývoje IS.
Podcenění uvedených oblastí ze strany kompetentních a odpovědných zástupců zákazníka (v průběhu specifikace zadání, akceptace IS či zavádění IS do provozu) může snížit kvalitu rutinního provozu podnikového IS a zvýšit rizika plynoucí z provozu takového IS.

Literatura:

1. Shinder, D., L.: Počítačové sítě. Softpress s.r.o., Praha, 2003, ISBN 80-86497-55-0
2. Strebe, M., Perkins, CH.: Firewally a proxy servery. Computer Press, a.s., Brno, 2003, ISBN 80-7226-983-6
3. Rodryčová, D., Staša, P.: Bezpečnost informací jako podmínka prosperity firmy. Grada Publishing, s.r.o., Praha, 2000, ISBN 80-7169-144-5
4. Paleta, P.: Co programátory ve škole neučí. Computer Press, a.s., Brno, 2003, ISBN 80-251-0073-1
5. Voříšek, J.: Strategické řízení informačního systému a systémová integrace. Management Press, Praha, 1999, ISBN 80-85943-40-9