

Požadavky na outsourcing

Brno, 21.6.2011

Ing. Jan Bukovský, jan.bukovsky@ceb.cz



- **Outsourcing**
- firma vyčlení různé podpůrné a vedlejší činnosti a svěří je smluvně jiné společnosti (=poskytovateli outsourcingu), specializovanému na příslušnou činnost. Činnost není zajišťována vlastními zaměstnanci firmy, nýbrž na základě smlouvy. Outsourcing má vést :
 - ke snížení nákladů nebo
 - k soustředění na hlavní činnosti firmy
- **Offshoring**
- offshoring znamená přesun výroby do zahraničí bez ohledu na to, zda výrobu provádí jiná firma (pak jde zároveň o outsourcing) nebo jde pouze o přestěhování vlastní továrny (obvykle z důvodu využití daňových úlev nebo menší ceny práce)
- **Outplacement**
- v tomto smyslu jde o vyvedení části firmy (včetně zaměstnanců) do nové společnosti, nejčastěji s cílem šetřit mzdové náklady

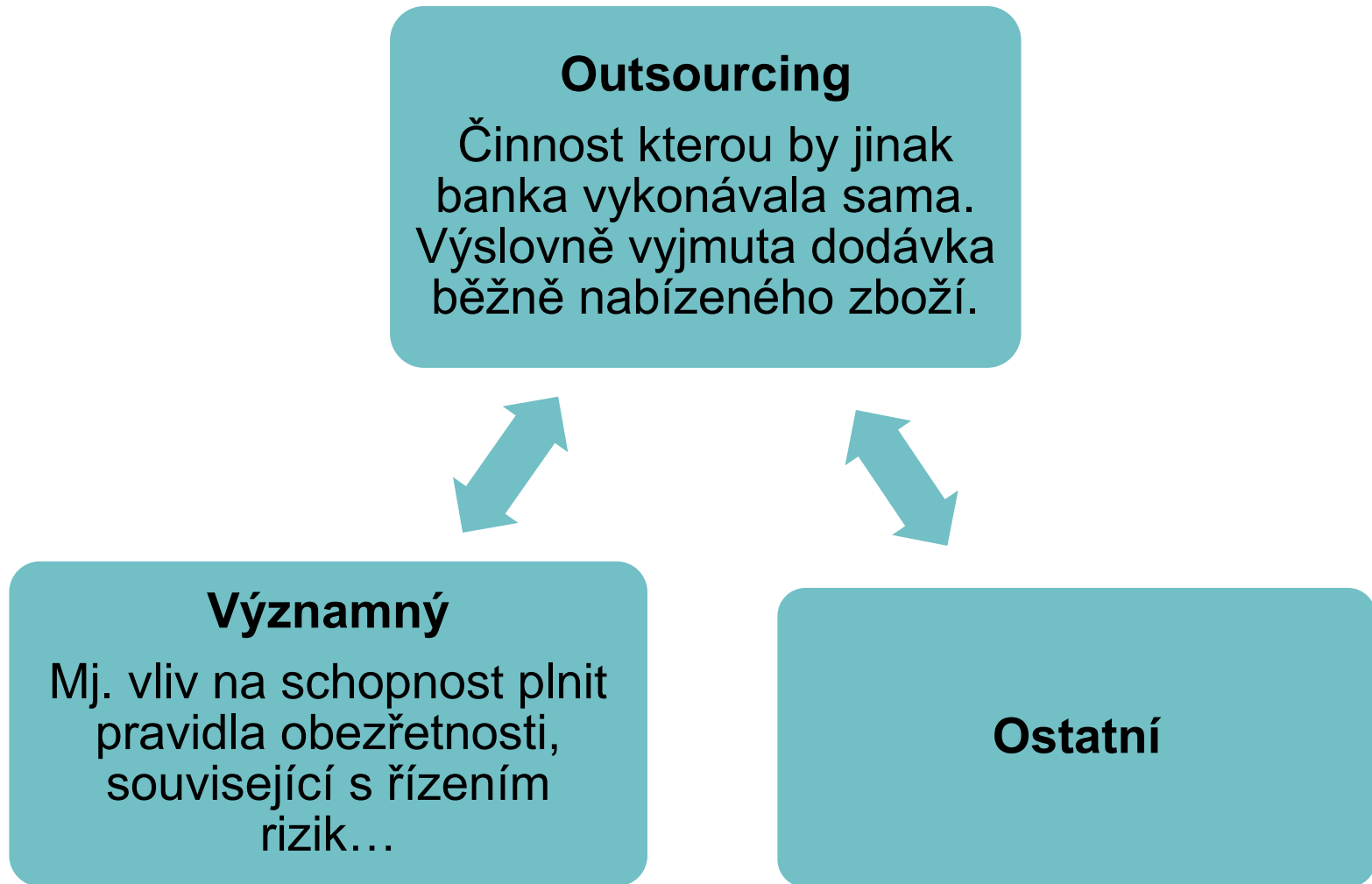


- **Cloud computing**
- Poskytování služeb či programů uložených na serverech na Internetu s tím, že uživatelé k nim mohou přistupovat prakticky odkudkoliv. Uživatelé neplatí (za předpokladu, že je služba placená) za vlastní software, ale za jeho užití.
- IAAS - infrastruktura jako služba - poskytovatel služeb se zavazuje poskytnout infrastrukturu. IAAS je vhodné pro ty, kteří vlastní software (či jejich licence) a nechtějí se starat o hardware.
- PAAS - platforma jako služba - poskytovatel v PAAS modelu poskytuje kompletní prostředky pro podporu celého životního cyklu tvorby a poskytování webových aplikací a služeb plně k dispozici na Internetu, bez možnosti stažení softwaru. To zahrnuje různé prostředky pro vývoj aplikace, ale také např. pro údržbu.
- SAAS - software jako služba - aplikace je licencována jako služba pronajímaná uživateli. Uživatelé si tedy kupují přístup k aplikaci, ne aplikaci samotnou. SaaS je ideální pro ty, kteří potřebují jen běžný aplikační software a požadují přístup odkudkoliv a kdykoliv.
- **Všechny typy cloud computingu (možná kromě SAAS) splňují definici outsourcingu dle ČNB („činnost, kterou by jinak vykonávala banka“.)**

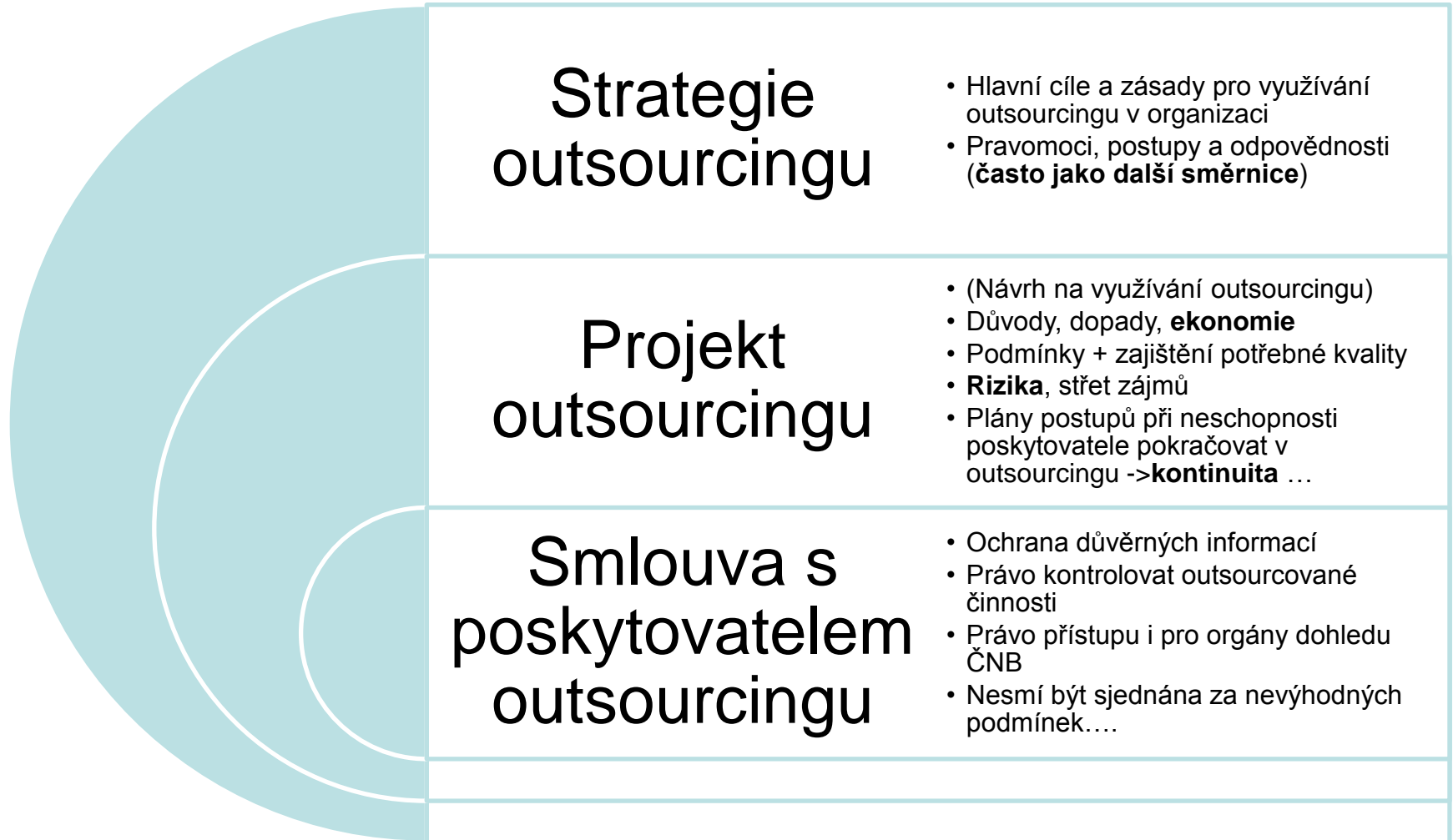


- **Hosting**
- Pronájem prostoru na cizím serveru (typicky např. webhosting)
- **Multihosting** - hosting většího počtu domén.
- **Virtuální server** - virtualizovaný stroj, který nabízí velkou konfigurovatelnost a větší výkon.
- **Managed server** - poskytovatel pronajme zákazníkovi vlastní server, o který se zároveň stará technická podpora poskytovatele. Jedno z finančně nejnáročnějších řešení.
- **Dedikovaný server** - podnájem serveru, který spravuje sám zákazník.
- **Hosting přerůstá v IAAS**. Rozdíl je hlavně v tom, že za hosting se hradí cena pouze v závislosti na velikosti pronajatého prostoru a dalších služeb, a u cloudu (IAAS) se hradí ceny podle rozsahu skutečně uskutečněných přístupů (při minimálním provozu=výrazně menší cena).





- Využitím outsourcingu se banka nezavazuje žádné ze svých odpovědností a
- Povinností dodržovat právní předpisy a
- Nepoškozovat zájmy třetích stran (vč. ochrany bankovního a dalších tajemství)!
- Proti starší úpravě se nerozlišuje jednorázovost / trvalost vykonávaných činností.
- Ohlašovací povinnost: O sjednání **outsourcingu významných činností** podle § 216 Vyhlášky musí být bez zbytečného odkladu informována ČNB.
- Řetězový outsourcing



- zda je outsourcovaná činnost trvale vykonávána v souladu se všemi příslušnými právními předpisy a se smlouvou,
- zda je poskytovatel outsourcingu nadále důvěryhodný a právně, finančně, odborně i technicky způsobilý k zajišťování outsourcovaných činností,
- zda poskytovatel outsourcingu pravidelně prověřuje funkčnost a dostatečnost svých mechanismů vnitřní kontroly a řízení rizik včetně řízení rizika výskytu mimořádných událostí a zda má vytvořeny dostatečně kvalitní postupy pro zajišťování outsourcované činnosti,
- zda nedochází ke změnám rizik spojených s outsourcovanou činností proti původním předpokladům,
- zda je ochrana bankovního tajemství, obchodního tajemství a osobních údajů klientů trvale a dostatečně zajištěna,
- zda jsou dodržovány vnitřní zásady a postupy banky pro outsourcing,
- zda vnitřní kontrolní mechanismy banky a poskytovatele outsourcingu zajišťují včasné zjištění případných nedostatků při využívání outsourcingu a přijetí opatření k nápravě,
- Zda celková funkčnost a efektivnost outsourcingu, rozsah a kvalita odvedené činnosti odpovídá předpokladům.



Jako možná operační rizika specifická pro poskytovatele outsourcingu jsou identifikována zejména:

- významné změny podmínek, například finanční situace, organizačního nebo vlastnického uspořádání, na straně poskytovatele outsourcingu,
- významné změny podmínek, například právních, v zemi sídla poskytovatele outsourcingu,
- nadměrná koncentrace v souvislosti s outsourcingem na straně poskytovatele posuzovaná pro případ, že tento poskytovatel by selhal a banka by byla vystavena většímu riziku nezajištěných činností. Pro případ, že by k tomu došlo, musí mít banka připravený odpovídající pohotovostní plán, jak činnosti realokovat na jiného (jiné) poskytovatele bez narušení plynulosti činnosti a nadměrných nákladů,
- Problémy z pohledu cloud computingu:
 - Často cizí legislativa, právní podmínky poskytovaných služeb tudíž nejasné
 - Banka by neměla být odkázána výhradně jen na hosting, aby naplnila podmínky ČNB o bránění nadměrné koncentraci
 - Obtížné využít např. pro platební styk (zákon ukládá odpovědnost za zabezpečení plně bance, což je obtížné garantovat na cizím řešení)
 - Obtížnější náhrada při selhání dodavatele



- Outsourcing – vyčlenění těch činností mimo vlastní organizaci, jejichž realizace vlastními silami je neefektivní.
- Projekty ISVS musí být koncipovány, aby umožnily případné využití outsourcingu.
- Přitom se přímo zmiňují projekty IS týkající se:
 - Akvizice
 - Vývoje
 - Provozu
 - Údržby.
- (ISO6/2000)



- A.6.2.1 Identifikace rizik plynoucích z přístupu externích subjektů
- *Předtím, než je externím subjektům povolen přístup k informacím organizace a prostředkům pro zpracování informací musí být identifikována rizika a implementována vhodná opatření na jejich pokrytí.*

- A.6.2.2 Bezpečnostní požadavky pro přístup klientů
- *Předtím, než je klientům umožněn přístup k informacím a aktivům organizace musí být zjištěny veškeré požadavky na bezpečnost.*

- A.6.2.3 Bezpečnostní požadavky v dohodách se třetí stranou
- *Dohody uzavřené s třetími stranami zahrnující přístup, zpracování, šíření nebo správu informací organizace nebo správu prostředků pro zpracování informací (případně dodávku produktů nebo služeb k zařízení pro zpracování informací) musí pokrývat veškeré relevantní bezpečnostní požadavky.*



- A.10.6.2 Bezpečnost síťových služeb
- Musí být identifikovány a do dohod o poskytování síťových služeb zahrnuty bezpečnostní prvky, úroveň poskytovaných služeb a požadavky na správu všech síťových služeb a to jak v případech, kdy jsou tyto služby zajišťovány interně, tak i v případech, kdy jsou zajišťovány cestou outsourcingu.

- A.10.8.2 Dohody o výměně informací a programů
- Výměna informací a programů musí být založena na dohodách uzavřených mezi organizací a externími subjekty.

- A.12.5.4 Únik informací
- Musí být zabráněno úniku informací.

- A.12.5.5 Programové vybavení vyvíjené externím dodavatelem
- Vývoj programového vybavení externím dodavatelem musí být organizací dohlížen a monitorován.



- Ekonomická výhodnost
- Zajištění kvality
- Analýza rizik a opatření k jejich odstranění
- Zabránění střetu zájmů
- Nesmí omezovat soulad činnosti s právními předpisy
- Ochrana důvěrných informací
- Zajištění požadavků na bezpečnost
 - Včetně bezpečnostních zásad obsažených již ve smlouvě
- Smlouva za výhodných podmínek
- Podmínky u dodavatele (kontrolní systém, směrnice...)
- Zabránění nadměrné koncentraci
- Provádění kontroly u poskytovatele outsourcingu a její pravidla
- Informační povinnost poskytovatele (cokoli, co by mohlo omezit jeho schopnost poskytovat outsourcing)
- Řetězový outsourcing nebude v rozporu se smlouvou o outsourcingu
- Oprávnění požadovat nápravná opatření / sankce
- Pravidla pro řízení kontinuity



- Outsourcing je ve skutečnosti ekonomicky nevýhodný
- Kvalita činnosti poklesla po přechodu na outsourcing
- Outsourcing přináší nová rizika, proti nimž se společnost nebrání
- Data nejsou dostatečně chráněna; hrozí spory s třetími osobami kvůli prolomení tajemství
- Poskytovaný outsourcing není v souladu s českým právem nebo představou nadřízených / kontrolních orgánů
- Bezpečnost nezajištěna (bezpečný přenos, bezpečné úložiště, otestované aplikace...)
- Organizace se stane na poskytovateli nadměrně závislá a v případě náhlého ukončení nebo omezení jeho činnosti jej není možno ihned nahradit
- Poskytovatele nikdo nekontroluje, faktury se proplácejí automaticky, nikdo nezná reálný stav u poskytovatele (často se uláže, že jde ve skutečnosti o řetězový outsourcing, o němž zadavatel vůbec nemá ponětí)

- Proti běžnému outsourcingu má cloud i některé další nevýhody, např.:
 - Slabší transparentnost (pro objednatele „černá skříňka“),
 - Slabší soulad s českým právem.
 - Právní otázky kolem vlastnictví dat a duševního majetku,
 - Obtížný přístup k logům a vyšetřování nevhodné nebo nezákonné činnosti,
 - Omezená rychlost a dostupnost ,
 - Náklady na širokopásmové připojení a další servisní náklady ,
 - Problémy v přenositelnosti dat na jinou platformu,
 - Riziko ztráty dat v případě chyby poskytovatele (ani zálohování není v rukách objednatele).



Děkuji Vám za pozornost...

Ing. Jan Bukovský, jan.bukovsky@ceb.cz

