Cloud nejsou jen superlativa

Jan Šeda

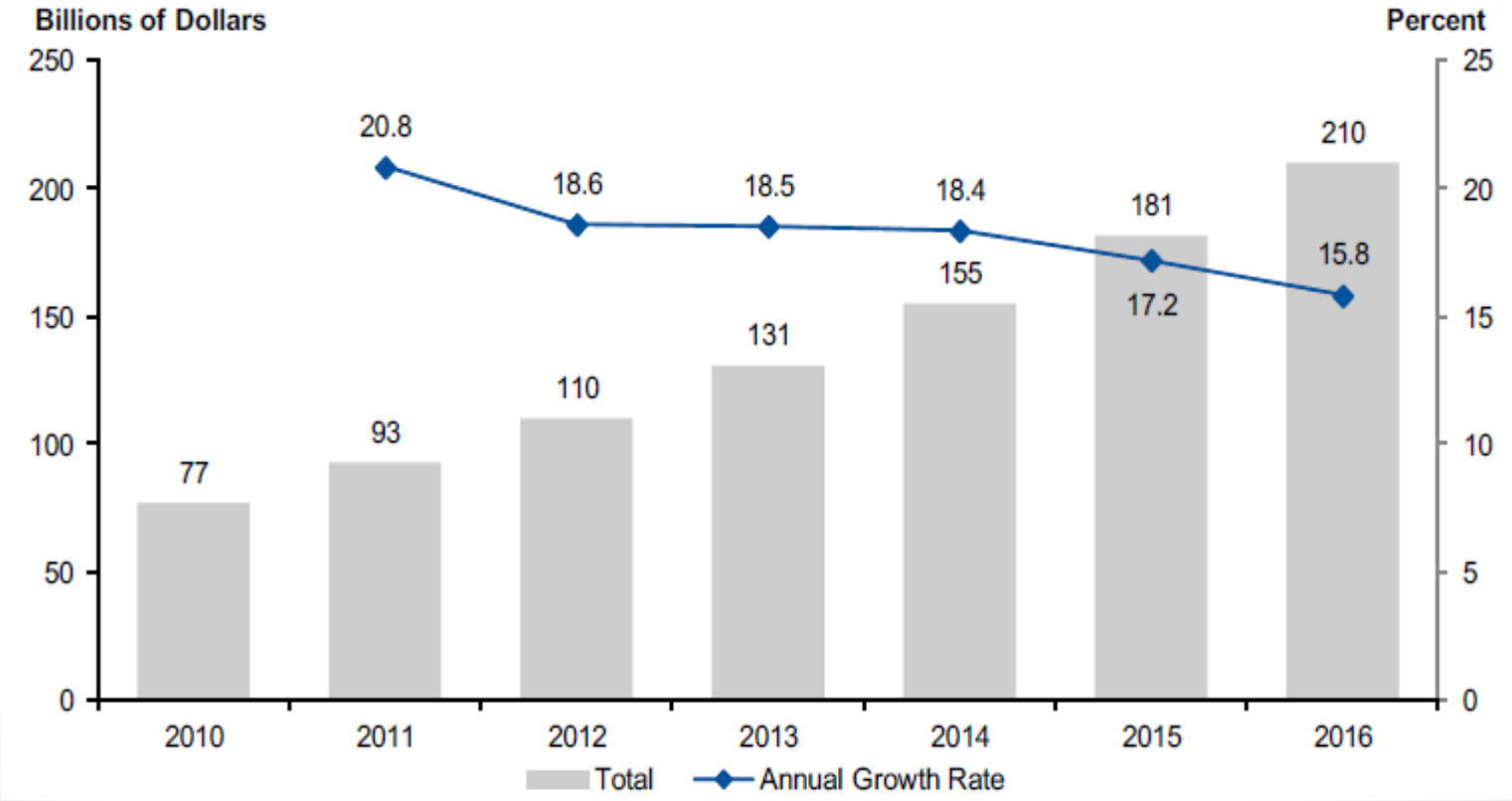
Mathix
Advokátní kancelář Dvořák Hager & partners

Proč používat cloud?

- Veřejný, privátní a hybridní
- Různé modely jeho využití: SaaS, IaaS, PaaS, SaaS, NaaS
  - Existují submodely podle typu odvětví (reklama, gaming, ERP atd.)
- Výhody cloud řešení
  - Centralizované řešení a správa = snížení nákladů díky nižší redundanci
  - Velmi dobře měřitelné a optimalizovatelné KPI
  - Zvýšení spolehlivosti (ne vždy)
  - Konsolidace výkonnostních prostředků
  - Vyšší kvalifikace personálu (měla by být), ale nižší náklady (menší počet IT zaměstnanců)
  - Soutředění se na hlavní byznys (ICT a hlavně infrastruktura je v mnoha subjektech podpůrná)

Public cloud roste

- Okamžitá úspora a marketing vede k jeho růstu
- Public cloud v roce 2012 obrat 110mld USD z toho 52% připadá na reklamu (v roce 2016 to má být 46% - 310mld USD)
- Nejvíce rostla public cloud reklama – 48% v 2012
- Model IaaS ve 2013 růst 47%, mělo by dojít ke zrychlení, roste gaming sektor
- Do roku 2016 má public cloud představovat v součtu objem obchodu 677mld USD



Někdy býti skeptikem

- Jde o naše data a to jsou naše peníze = vyhodnocení rizik
- Cloud = outsourcing ICT a sofistikovaný hosting
  - Je nutné jej takto hodnotit a vycházet ze stejných zkušeností a právních principů
- Centralizované řešení = centralizované riziko
  - Maličká chyba má obrovský dosah, viz. chybné smazání dat na LB serveru AWS = velké servery šly dolů*
- 100% užití cloud = 100% důvěra a odevzdání se poskytovali
- Decentralizace a distribuce jsou v mnoha faktorech výhodné (bezpečnost, stabilita, diverzifikace)
- Úspora může být velmi drahá – viz. dále
- Důvěřuj, ale prověřuj
  - Cloud Security Alliance
  - sada norem ISO/IEC 27000 (hlavně ISO/IEC 27002)

- http://www.inquisitr.com/463312/netflix-outage-was-caused-by-deleted-amazon-web-services-data/

Ochrana osobních údajů

- Týká se mě to? Pokud nevyužíváte internet tak ne ☺
- Směrnice 2009/136/EC novelizuje 2002/58/ES a ta doplňuje směrnici 95/46/ES
  - Bird & Bird – není implementována vs. ÚOOÚ – je implementována
  - http://www.samoregulace.cz/sites/default/files/cookies_vcr.pdf
  - Oznamovací povinnost provozovatele vůči ÚOOÚ při zpracování cookies
  - Zatím je situace velmi nejasná
    - EU nevádá žádné výkladové stanovisko (jedná se o směrnici -> vše přenáší na státy)
    - Orgány členských států nevědí, jak má být implementována => co má dělat provozovatel?
- Důležitý právní spror: je jednání uživatele opt-in a nebo opt-out?
  - Implicitní nastavení prohlížeče je *souhlas*?

  nebo Implicitní nastavení není *aktivní souhlas*?
- Sledování a detekce osobních dat na cloud systémech
  - Skydrive*
  - Automatizované elektronické systémy s nejasnými následky pro uživatele (monitoring dat a blokování účtu)
- Která juridiskce je uplatňována?
  - Každý z údajů ma jiný právní výklad (také je otázkou, který podléhá regulaci a který ne – viz příklad s cookies UK, ČR a Německo)
- Osobní údaje je možné dolovat přes Google Code Hacking**

- *http://www.lupa.cz/clanky/jak-microsoft-bojuje-proti-nahote-na-privatni-skydrive-nesmi-ani-kreslene-nadro/
- **Http://www.darkreading.com/cloud-security/167901092/security/vulnerabilities/231902718/cloud-services-credentials-easily-stolen-via-google-code-search.html

Dojmy versus Pojmy

- Dojmy – emoce namísto objektivity
  - Subjektivní emoce namísto objektivních faktů
  - Velká firma = vše funguje dobře
  - Mají nejlepší lidi
  - Mají hodně peněz, tak to nějak zařídí
  - Jsou lepší než já (Sybase a „bílé pláště“)
- Realita
  - Velká firma = velký cíl
  - Obvykle vůbec nic nevíme o vnitřních procesech a standardech, většina je tajná
  - Známe veřejně známé osoby, evangelizátory, ne „dělníky“ na pozadí
  - Hodně peněz, ale žádná firma nepublikuje detailní rozpočet a nikde nevíme, kolik z těch „hodně peněz“ se dotýká nás
  - Někdy neuškodí trocha toho zdravého seběvědomí, ale zdravého! ☺
- Být realista – nejednat podle marketingu, ale mít zdravý selský rozum
- Zkoumat reference a zkušenosti ostatních

Dojmy versus Pojmy II

- Namátkové případy průniků a výpadků enterprise cloud subjektů
  - Google (01/2010): http://www.ft.com/cms/s/2/2eda6f70-0059-11df-8626-00144feabdc0.html#axzz2NYbMd3sg
  - Amazon Web Services (05/2011): http://www.zdnet.com/amazon-cloud-used-in-playstation-network-hack-4010022454/
  - DropBox (09/2012): http://www.zdnet.com/dropbox-gets-hacked-again-7000001928/
  - Amazon Web Services (10/2012): http://www.pcworld.com/article/2012852/amazon-web-services-outage-takes-out-popular-websites-again.html
  - Amazon Web Services (24/2012): http://www.wired.com/wiredenterprise/2012/12/amazon-outag/
  - Evernote (02/2013): http://www.engadget.com/2013/03/02/evernote-hacked/
  - Amazon Web Services (01/2013): http://www.wired.com/wiredenterprise/2013/01/amazon-down/
  - Facebook (02/2013): http://edition.cnn.com/2013/02/15/tech/social-media/facebook-attack/index.html
  - Apple (02/2013): http://edition.cnn.com/2013/02/19/tech/web/apple-hacked
  - Microsoft Azure (02/2013): http://www.latimes.com/business/technology/la-fi-tn-microsoft-hack-azure-20130222,0,6681241.story

Konkrétní příklady z praxe I

- Příklad 1 – klient v ČR + poskytovatel v ČR
  - Provoz public cloud řešení od roku 2010
  - Nedostupnost v důsledku automatických změn v operačním systému (povolena automatická bezpečnostní aktualizace)
  - Provozovatel nabízí pouze cenově nepřijatelné řešení
  - Spor o pojem dostupnost a zavinění
  - Hledání dohody => 24 hodin nekontrolovaný systém
    - Nedostupná odpovědná osoba mimo mobil (víkend a druhý dovolená)
    - Chybně definovaná zastupitelnost ze strany poskytovatele - klient nezjistí do doby výskytu incidentu
    - Podezření na průnik a následná dohoda o uhrazení zásahu (délka trvání zásahu 1-2 minuty)
  - Výsledkem jednání o změnách smluv a vydefinování si scénáře migrace k jinému poskytovateli
  - Škody:
    - Fulltime čas jednoho člověka ze strany klienta a přímé platby poskytovali
    - Požadavek na navýšení ceny za vyšší garance ze strany poskytovatele
    - Ztráty v důsledku výpadku systému
    - Systém bez jakékoliv kontroly po dobu 24h

Konkrétní příklady z praxe II

- Příklad 2 – klient v ČR + poskytovatel v zahraničí
  - Klient provozující vlastní CRM řešení pro outsourcing call centra
  - Migroval do SaaS modelu CRM provozovaného na zahraničním poskytovateli cloud infrastruktury (virtulizované clustery serverů v USA)
  - Interní vývojový tým byl po půl roce úspěšného provozu cloudu zrušen (úspora 2 FTE)
  - V roce 2009 došlo k překopnutí kabelu UPC => extrémmí zpomalení provozu a ochromení call centra
  - Celodenní výpadek a fungování call centra v modelu „chaos“ a snaha o instalaci původního systému v době výpadku
  - Škody:
    - Penalizace call centra ze strany objednatelů jeho služeb
    - Náklady na přesčasy zaměstnanců na přepis papírových dokumentů do elektronické podoby
    - Náklady na zpětný přesun CRM do místa působiště klienta

Cloud Escrow

- Riziko výpadku cloud služeb => vznik služeb cloud escrow
  - Cloud Escrow = Business Continuity
- Vytváří se mezičlánek mezi klientem a poskytovatelem cloud služby
  - Cloud Escrow drží zdrojové kódy a dokumenty ve dvou geograficky a technicky nezávislých oblastech
  - Vše je vydáno klientovi v momentě, kdy dojde k výpadku
  - Může být zajištěno i obnovení služby, ale cloud escrow je více ve formě notářského zajištění
- Velmi ranná fáze vývoje
  - Zatím málo výhod pouze při využití cloudu
  - Fungovaje v kombinaci outsourcing vývoje + cloud služby => zajištění třetím právním subjektem vůči dodavatelům
- Existence této služby dokazuje rizika cloudu a potřebu je řešit
- Cloud Escrow Alliance nemá mezinárodní charakter (jen v EU)

To Cloud or not to Cloud?

- Cloud je technicky vynikající řešení, ale ...
- Ke cloudu je nutné přistupovat stejně jako k libovolné službě třetí strany (outsourcing, hosting atd.)
- Stanovení si důležitosti ICT pro společnost (váhování stejně jako při outsourcingu ICT, pokud jeho důležitost ve firmě není zásadní)
  - Pokud firma odmítá outsourcing => veřejný cloud je automaticky ze hry
- Stanovení si jasných očekávání od cloud
  - Snížení nákladů je nedostatečné hodnocení
  - Rozsah aplikací
  - Kategorizace dat a jejich právní posouzení (regulace, rizika, povinnosti správce a nakládání s daty, zákon 499/2004 Sb.)
- Po evaluaci využití cloud služeb volba mezi veřejným, privátním a hybridním
- Kvalitní SLA
  - Investice do kvalitního právního zhodnocení se zde určitě vyplatí
  - Tuto problematiku řešíme s advokátní kanceláří Dvořák Hager& partners (www..akds.cz)
  - Jasná specifikace pojmů jako dostupnost, auditing a jasné vymezení odpovedných osob
  - Vydefininování klíčových a rizikových situací a optimálně i postup řešení (výpadek, stanovení odpovědnosti po následném vyřešení, stanovování si rizik a priorit atd.)
  - Stanovení si řešení výpadků, přesuny, komunikace, notifikace
- Zvážit investice do produktů jako Veeam na zálohování a replikace, případně podobných technické ochrany jako dvoufázovou autentikaci a komplexní zavedení PKI
  - Může představovat zdrojený náklady díky faktické realizací hybridního cloudu
- Podle povinností s nakládáním s daty stanovit a zjistit, který poskytoval dokáže splnit podmínky
  - Audit osob s přístupem ke zdrojům HW i SW
- Způsoby a důvody ukončení služby a forma a způsob předání majetku klienta

Otázky

Na přelomu 03/04 2013 Cloud Security Workshop