Sdílené ICT služby a G-cloud v české veřejné správě

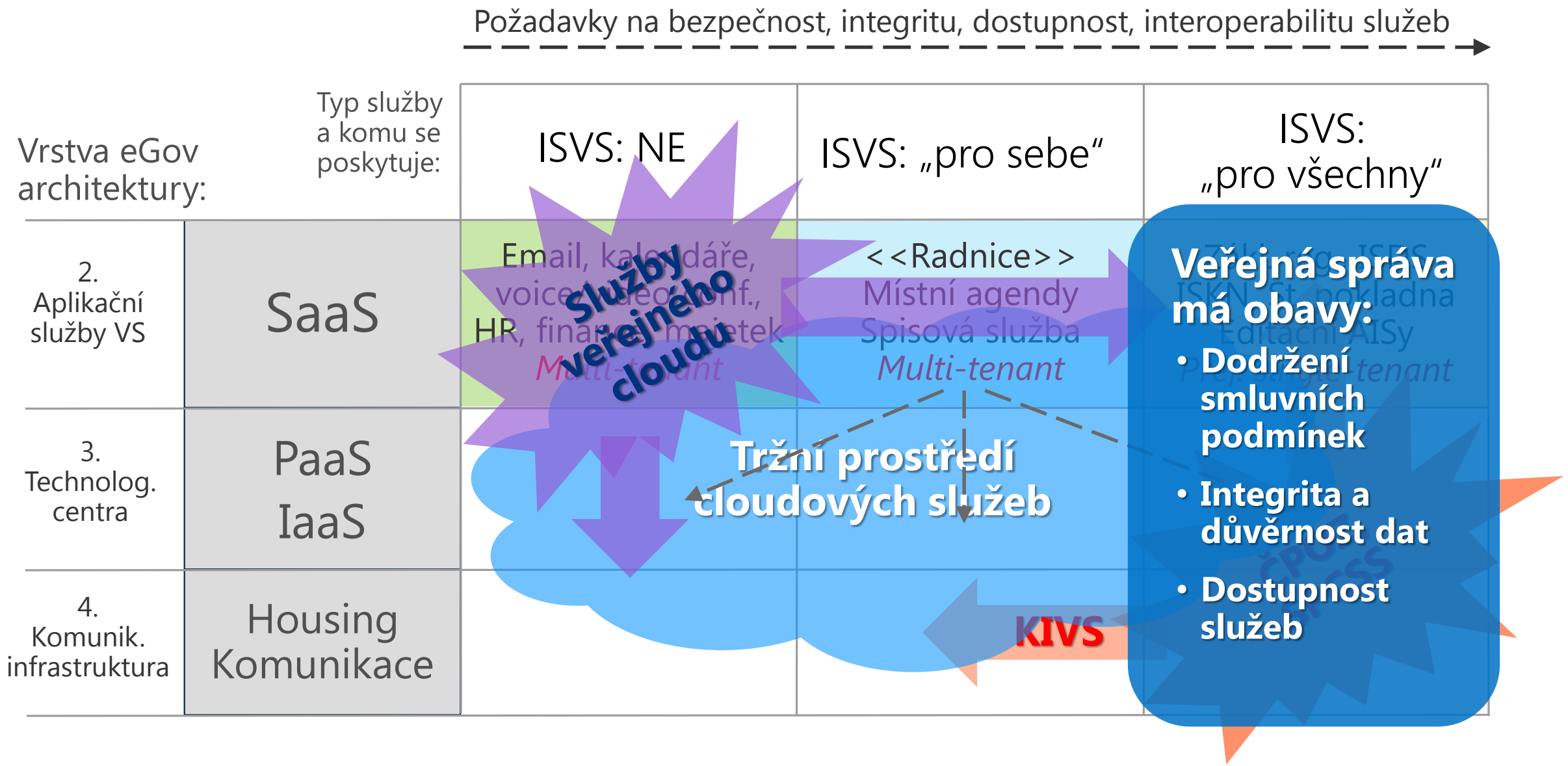
Ing. Zdeněk Jiříček, Ing. Václav Koudele

O čem budeme hovořit

- Sdílené služby od komerčních dodavatelů
- Odstupňování požadavků na sdílené služby
- Jak nakupovat sdílené služby
- Způsoby pojetí zajišťování sdílených služeb
- Katalog sdílených služeb

Cloud first

Návrh metodiky využití sdílených služeb pro VS



Východiska pro akreditační požadavky

Zákon o ISVS č. 365/2000 Sb. a jeho vyhl. č. 529/2006

- Pouze obecné požadavky na důvěrnost, integritu a dostupnost
- Bezpečnostní dokumentace: bezp. politka, bezp. směrnice.... (potřebuje aktualizaci)

Zákon o ochraně osobních údajů č. 101/2000 Sb.

- §6 – Smluvní vztah mezi správcem a zpracovatelem
- §13 - Analýza rizik => smluvní záruky zavedení bezpečnostních opatření
- §27 – Předání dat do jiných zemí - podmínky uložení a zpracování dat v cloudu

Zákon o kybernetické bezpečnosti č. 181/2014 Sb.

- Vymezit ISMS, aktiva, analýza rizik => bezpečnostní opatření, smluvní záruky

Soulad cloudových dodávek dle vyhl. č. 316/2014 Sb.

Dle §7 – Bezpečnostní požadavky pro dodavatele povinných osob

„VIS“ – pouze odst. (1)

Požadavek zavedení pravidel pro dodavatele pro potřeby řízení bezpečnosti informací

Dokumentaci provést smlouvou, jejíž součástí je ustanovení o bezpečnosti informací

Výčet opatření zahrnout do smluvních podmínek

„KII“ – dále odst (2) b

Smlouva zahrnuje způsoby a úrovně bezp. opatření a vztah odpovědnosti za jejich zavedení a kontrolu

Výčet opatření zahrnout do smluvních podmínek

Předat povinné osobě podklady:

1. Bezpečnostní politiku dodavatele
2. Certifikát ISO 27001
3. ISO 27001 prohlášení o aplikovatelnosti (plná struktura bezpečnostních opatření)
4. Auditní zprávy ISO 27001, případně SOC 1 & 2

„KII“ – dále odst. (2) a, c

Pravidelné hodnocení rizik služeb (příp. i před uzavřením smlouvy); Kontroly zavedených bezp. opatření

Předat povinné osobě podklady:

1. Metodika hodnocení rizik, včetně proměnných a jejich úrovní (Příloha 2)
2. Min. seznam hrozeb a zranitelností (§4)
3. Závazek včasného řešení vyšších úrovní výsledných rizik (Příloha 2)
4. Pravidelnost procesů hodnocení rizik a hierarchie jejich akceptace (Příloha 2)

Kontrola účinnosti zavedených bezp. opatření auditními zprávami ISO 27001 a SOC 1 & 2 Type II

Řízení rizik + ISO 27001:2013 bezpeč. opatření

Bezpečnostní opatření

Řízení rizik

Hrozby + Zranitelnosti

Aktiva

1. (A.05) Bezpečnostní politika
2. (A.06) Organizační bezpečnost
3. (A.07) Bezpečnostní požadavky na dodavatele
4. (A.08) Řízení aktiv (obsahuje požadavky na ochranu dat)
5. (A.09) Bezpečnost lidských zdrojů
6. (A.10) Řízení provozu a komunikací
7. (A.11) Řízení přístupu
8. (A.12) Akvizice, vývoj a údržba
9. (A.13) Zvládání bezpečnostních incidentů
10. (A.14) Řízení kontinuity činností
11. (A.15) Kontrola a audit
12. (A.16) Fyzická bezpečnost a vliv přírodních rizik
13. (A.17) Integrita kom. sítí
14. (A.18) Ověřování identity uživatelů
15. (A.19) Řízení přístupových oprávnění
16. (A.20) Ochrana před škodlivým kódem
17. (A.21) Nástroje pro logování činností
18. (A.22) Nástroje pro detekci událostí
19. .....
20. (A.25) Kryptografické prostředky

Shrnutí požadavků pro akreditační proces

Požadavky na bezpečnost, integritu, dostupnost, interoperabilitu služeb

ISVS: NE	**ISVS: „pro sebe“**	**ISVS: „pro všechny“ (ze zákona)**
Osobní údaje NE: Pouze smluvní podmínky Smlouva o úrovni služeb (SLA) **Interop:** výměnné formáty	**Vždy:** Smluvní podmínky Smlouva o úrovni služeb (SLA) Bezpečnostní politika **Interop:** navíc Interconnect (CMS)	Smluvní podmínky s vysokou vymahatelností SLA s vysokými parametry **Interop:** navíc Interconnect, eIDAS
Osobní údaje ANO: §6 Záruky zabezpečení ochrany osobních údajů ve smlouvě §13 Analýza rizik, prokazatelné zavedení bezp. opatření §27 Ošetřit předání dat do jiných států		**Osobní údaje ANO (velký objem?):** Navíc: Úroveň auditní zprávy
VIS ? Oblastní a dopadová krit. (el. pošta, internet. stránky) Malá pravděpodobnost zařazení do VIS	**VIS:** Prokazatelné zavedení bezp. opatření dle ISO 27001:2013 **KII:** navíc dokumentace pro analýzu rizik dodavatele	**VIS:** Prokazatelné zavedení bezp. opatření dle ISO 27001:2013 **KII:** navíc dokumentace pro analýzu rizik dodavatele

Efektivita multi-tenantních služeb

- **Úroveň SaaS, výhody oproti single-tenantním**
- **Výrazně efektivnější u komoditních a vícenásobně využívaných sdílených služeb**
- **Příklad – poštovní server jako služba?**
  - **Náklady single-tenantního řešení**
    - **Individuální náklady -** implementace, správa, údržba
    - **„Nákladově rozpuštěno“ mezi všechny zákazníky -** Sdílená IaaS
  - **Náklady multi-tenantního řešení**
    - **Individuální náklady -** implementace
    - **„Nákladově rozpuštěno“ mezi všechny zákazníky -** Sdílená SaaS, správa, údržba

Jak nakupovat cloudové služby?

Technologicky neutrální kritéria pro cenové srovnání infrastrukturních služeb IaaS/PaaS

- Každý poskytovatel cloudových služeb má jinak diverzifikovaný produkt – i přesto lze porovnávat
- Volba optimálního zadání dle technických kritérií (nejmenší společný jmenovatel)
  - Spotřeba měřena po hodinách
  - Minimální rozsah požadovaných funkcionalit
  - Minimální rozsah dostupných konfigurací pro VM
  - Požadovaná SLA

Požadavek:	**Virtuální servery s předinstalovaným operačním systémem následujících HW konfigurací**
Specifikace	Virtuální servery pro platformy **SUSE Linux Enterprise Server 12, SUSE Linux Enterprise Server 11 SP3, Windows Server 2012 Datacenter, Windows Server 2012 R2 Datacenter, Windows Server 2008 R2 SP1, Ubuntu Server 14, Oracle Linux 7** pro následující hardwarové konfigurace: **Servery standardní** 0,25 jádra, 0,75 GB RAM; 1 jádro, 1 GB RAM; 2 jádra, 2 GB RAM; 2 jádra, 4 GB RAM; 4 jádra, 8 GB RAM; 8 jader, 14 GB RAM **Servery s podporou vysoké dostupnosti** a load balancingu (Load Balancing, Automatická reakce na výkonový požadavek) 2 jádra, 3,5 GB RAM, 8 jader, 14 GB ;8 jader, 56 GB **Servery s podporou vysokého výkonu** (Load Balancing, Automatická reakce na výkonový požadavek) 8 jader, 28 GB, 400 GB local SSD cache; 16 jader, 112 GB, 800 GB local SSD cache Zadavatel požaduje alespoň 20 hardwarových konfigurací. Zadavatel připouští i jiné HW konfigurace, než uvedl v této tabulce, ale trvá na minimální konfiguraci (0,25 jádra, 0,75 GB RAM) a maximální konfiguraci (16 jader, 112 GB, 800 GB local SSD cache, Load Balancing, Automatická reakce na výkonový požadavek). Ostatní konfigurace mohou být navrženy uchazečem tak, aby se odchylovaly směrem k vyšším parametrům od požadovaných konfigurací v této tabulce max. o 20%. Rozdíl směrem k nižším parametrům není přípustný.
Rozsah dostupnosti	Minimálně 500 serverů
Přípustný čas pro zprovoznění služby	Maximálně 10 min

Inspirace: PIERSTONE

http://pierstone.com/vzorova-zd-na-cloudove-sluzby-duben-2015/

Přínosy G-cloudu a cloudu veřejné správy uživateli

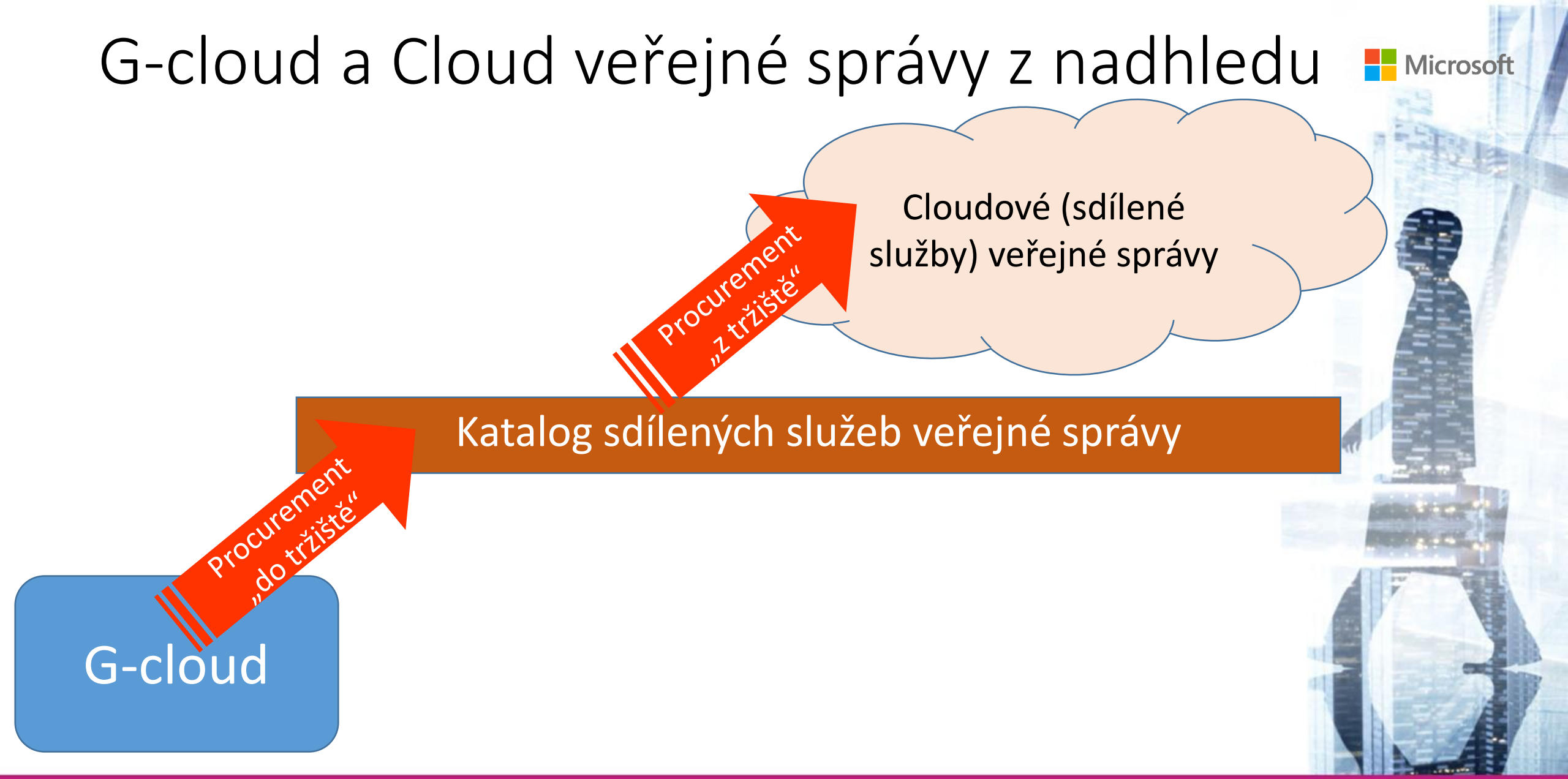
- Občanovi to je „jedno“ - uživatelé jsou subjekty veřejné správy

- Velký a střední úřad – IaaS, PaaS, SaaS
  - Vlastní lidské zdroje pro správu

- Malý úřad – spíše jen SaaS
  - Požadavek vše „na klíč“ a srozumitelně (balíčky SaaS) – benefit – multitenantní SaaS je ekonomicky výhodnější

G-cloud a Cloud veřejné správy z nadhledu

G-cloud a Cloud veřejné správy z nadhledu



Katalog sdílených služeb veřejné správy

- Místo, kde hledám sdílené služby
- Jak to vypadá z pohledu uživatele?
- Jak to vypadá z pohledu dodavatele?

Katalog z pohledu uživatele (OVM)

- Vazba na RPP – kategorizace sdílených služeb
- Po autentizaci vidím:
  - Co vykonávám jako úřad ze zákona
  - Co na to používám za informační systémy
  - Co mi chybí - jaké jsou možnosti sdílených služeb pro „neobsazené“ agendy

Katalog sdílených služeb veřejné správy

- Jak to vypadá z pohledu dodavatele?

G-cloud a Cloud veřejné správy z nadhledu

Microsoft

Katalog sdílených služeb veřejné správy

eGON pravidla

Hlavní architek eGOV

BluePrints – pro jednotlivé typy sdílených služeb definovat jistou úroveň požadavků na důvěrnost, integritu, dostupnost a interoperabilitu

IS na všechno

Nekvalitní dodavatel

AIS1

Dodavatel AIS I.

AIS2

Dodavatel AIS II.

Komoditní SS

Dodavatel komoditní sdílené služby

Od konceptu k optimální metodice

- Jak pomocí G-cloudu akcelerovat adopci a trh sdílených služeb…
  - Celý koláč ICT se přijetím sdílených služeb pravděpodobně zmenší – v multitenantní podobě to bude pravděpodobně levnější
  - Pravděpodobně bude trh sdílených služeb zvětšen o ty segmenty, kde díky neinformovanosti, nebo neefektivní implementaci on-premise řešení zatím žádní IS nebyl využíván

Od konceptu k optimální metodice

- Jak pomocí G-cloudu pokřivit trh ICT služeb
  - Vyberu tendrem na nejnižší cenu jednoho, který se zaváže ke splnění přísných požadavků, ale ukáže se v čase, že není schopen kontrahovanou službu dodat….
  - Ale ostatní dodavatelé přestali do tohoto segmentu trhu investovat.
  - Pravidlo rozumného minima vendorů - zachovat zdravé tržní prostředí

Poskytovat služby cloudu veřejné správy pro subjekty VS zdarma?

Na Slovensku je takto poskytován…

Jak v České republice?

Tragédie špatného cloudu veřejné správy

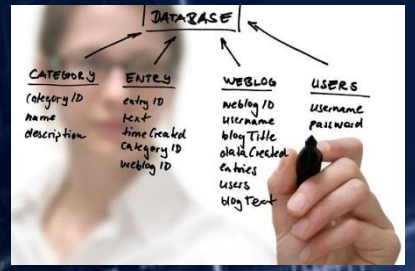
Para
Har

- Jakýkoliv výkon se vždy vyčerpá!
- Jakýkoliv diskový prostor se vždy zaplní!
- Pokud nejsme motivován k efektivnímu využívání sdílených prostředků, využíváme neefektivně!

…..
kteř
oso
důs
daného zdroje (erozi surovinové základny), a tedy ke snížení užitku všech jednotlivců…..

Kde již dnes využívají cloudové služby

Office365 v podmínkách MMHK, Statutární město Hradec Králové

Popis	• *Požadavek: cenově přístupné software assurance pro Office* • *Office365 splňuje, využit FastTrack program (implementace)*	
Přínosy	• *Instantní komunikace (menší zahlcenost maily, historie, přítomnost)* • *Office 2013 na více zařízeních (BYOD) včetně mobilních (náhrada HUP)* • *Vždy aktuální verze (problematické v případě on-premise)* • *Cloud – zálohování, velikost schránky*	
Způsob pořízení	• *Pořízeno formou VZ v rámci obnovy smlouvy Enterprise Agreement*	
Použité technologie	• *Fáze nasazení Office365 – Lync, Office 2013, Exchange online*	

Věstník veřejných zakázek Ministerstva pro místní rozvoj

Popis

- *Věstník je poskytován jako služba pro všechny zadavatele veřejných zakázek dle zákona 137/2006 Sb.*
- *Věstník provozuje koncesionář (nyní NESS Czech s.r.o.) na vlastní náklady a inkasuje poplatky za uveřejnění ve výši dle vyhlášky přímo od zadavatelů.*
- *Jádrem je webová aplikace www.vestnikverejnychzakazek.cz na platformě ASP. NET*
- *Otevřené rozhraní pro autorizované odběratele, rozhraní na věstník EU (TED).*
- *Provoz 24 x 7, zákonné lhůty na zveřejnění ve věstníku ČR i EU.*
- ***První „velká“ aplikace na MS Azure v ČR***

Přínosy

- *Time-to-market: poskytovatel se mohl soustředit čistě na vývoj řešení, infrastruktura byla k dispozici prakticky hned.*
- *Dostupnost: poskytovatel nemusí řešit zajištění provozu infrastruktury.*
- *Škálovatelnost a cena: platí se spotřebovaný výkon.*
- *Maintenance SW komponent: řeší poskytovatel „na pozadí“.*

Věstník veřejných zakázek Ministerstva pro místní rozvoj

Způsob pořízení	• *Veřejná soutěž o koncesi na 5 let*
Použité technologie	*Základní technologie* • *ASP .NET* • *MS SQL* *Cloudové služby* • *A1 Cloud Services, Geo Redundant Storage, SQL Azure Business 10 DU, Storage Transactions, Windows Azure Data Transfer Egress Zone 1* *Navazující komponenty* • *Billing Engine (interní vývoj, J2EE)* • *Rozhraní TED (SOAP)* • *Rozhraní pro autorizované uživatele (SOAP)*
Výkonové charakteristiky a požadavky	• *Měsíčně uveřejněno v průměru 4.400 formulářů (nové VZ, změny, zrušení, etc…)* • *Je vystaven zhruba stejný počet faktur, z toho 40% zasílaných elektronicky.* • *Největší uživatelská špička cca 08:00 až 10:00.*

Spisová služba pro veřejnou správu jako sdílená služba

Popis	• *Hostovaná elektronická spisová služba pro subjekty, jimž to ukládá zákon a pro ty, které to považují za přínos. Jednotná aplikace s aplikací onpremise.*
Přínosy	• *U zákazníka: nemusí pořizovat a udržovat infrastrukturu (servery HW, SW…) dostupné při splnění autentizačních podmínek odkudkoliv.*
Způsob pořízení	• *Předmětem nákupu je licence, která v sobě obsahuje náklady na MS Azure. Zpravidla se jedná o veřejnoprávního původce a předmětem poptávky je služba, tedy nikoliv investice.*
Použité technologie	• *Aplikace AthenA (Host AthenA) je webová aplikace na technologiích: MS .NET, MS Windows Server, MS SQL Server, MS Office.*

Závěr

- Sdílené služby je možné nakupovat od komerčních dodavatelů.
- Je nutné odstupňovat požadavky na sdílené služby.
- Nic nebrání nakupovat sdílené služby v režimu ZVZ.
- Zachovat tržní prostředí i ve sdílených službách.

Děkujeme za pozornost

zdenekj@microsoft.com
vaclavko@microsoft.com

Backup

Ochrana osobních údajů – zák. č. 101/2000 Sb.

§6 zák. č. 101/2000 Sb.
Požadavek na „Smlouvu o zpracování dat“:
- Rozdělení rolí „Správce“ a „Zpracovatel“
- Písemná smlouva, záruky zabezpečení
- Uložení dat v EU nebo mimo EU?
- Zpracování dat v EU nebo mimo EU?

§13 zák. č. 101/2000 Sb.
Správce a Zpracovatel dat provedou:
- Analýzu rizik,
- Příslušná technická opatření,
- Smluvně zamezí zneužití osobních informací

§27 zák. č. 101/2000 Sb.
Předání osobních údajů Zpracovateli: jen EU?
Mimo EU: Safe Harbour, Standardní sml. doložky
V případě použití **„standardních smluvních doložek EU“ není třeba žádat úřad o povolení,**
viz web ÚOOÚ… kdy není třeba žádat o povolení
(dole na stránce)

Závěr pro poskytovatele cloudu:
„Smlouva o zpracování dat“ se zahrnutím „Standardních smluvních doložek“ ve znění přesně dle Rozhodnuní 2010/87/EC představuje dostatečné právní záruky zpracování osobních údajů i mimo EU.

Podrobné vysvětlení ÚOOÚ ke cloudovým službám: „K právní ochraně osobních údajů při jejich předávání v rámci cloudových služeb“