V Praze, 25. listopadu 2015

Současný stav provozu datacenter a serveroven
Vyhodnocení dotazníku dle RVIS
Management summary

1. Úvod

Rada vlády pro informační společnost (RVIS) pověřila Státní pokladnu Centrum sdílených služeb, s.p. (SPCSS) provedením průzkumu napříč resorty státní správy monitorující stav data center v gesci státní správy ČR, a to zejména úroveň zabezpečení, jejich kapacitu, konektivitu a další vlastnosti a parametry.

SPCSS na základě zadání vypracovala dotazník „Datové centrum povinné parametry“ a požádala o jeho vyplnění všechna ministerstva a jejich podřízené organizace, jejíchž gesce je pro účely dotazníků relevantní. Sběr dat a následně vyhodnocení dotazníků zajistila SPCSS.

Cílem toho dokumentu je především zhodnotit situaci, identifikovat rizika a na základě zjištěných skutečností stanovit nejlepší strategii budoucího postupu a rozvoje datových center v gesci státu.
Agenda jednotného rozvoje státních datových center nabývá na významu především v souvislosti s rozvojem agendy G-Cloudu. Jednotná pravidla a parametry pro uchovávání státních dat nejen že eliminují rizika, která jsou s provozem datových center spojená, ale významnou měrou přispějí ke zvýšení elektronizace veřejné správy a pomohou přiblížit úroveň českého eGovernmentu blíže k evropským standardům.

Rizika spojená s vlastním provozem datového centra:

Základním rizikem, které doprovází uchovávání dat ve státní a veřejné správě je v prvé řadě absence koncepčního řešení rozvoje datových center a uchovávání státních dat jako celku. Jednotlivé subjekty státní a veřejné správy nemají dlouhodobě koncepčně vyřešen provoz, vybavení zabezpečení a rozvoj datových center jednotlivých resortů. Není tedy možné efektivně plánovat investice do datových center, HW a zabezpečení a citlivá data jednotlivých státních subjektů jsou de facto uchovávána v nevyhovujících prostorech a na zastaralé infrastruktuře. K dalším rizikům, která je možné v této agendě identifikovat, patří především nemožnost a počáteční nereálnost odhadu budoucí potřebné kapacity datového centra. Následně pak dochází k poddimenzování kapacity, nebo naopak ke zbytečně vynaloženým nákladům z veřejných rozpočtů. Provoz vlastního datového centra rovněž vyžaduje odborné personální zajištění, a především zvládnutí fyzické a logické bezpečnosti uložených dat. Tyto nároky mnohdy subjekty státní správy nejsou schopny plnit vlastní silou a dochází tak ke značným rizikům, která mohou mít za následek ohrožení celého datového fondu.

2. Oslovené subjekty

Mezi oslovenými subjekty bylo 14 ministerstev a vybrané podřízené a přímo řízené organizace, celkem bylo odesláno 57 dotazníků. Odpověď byla doručena od 43 subjektů. Návratnost dotazníků je tedy 75 %.

3. Základní údaje

Dotazník obsahuje parametrizovaná kritéria pro hodnocení datových center, která jsou v současné době vlastněná a užívaná jednotlivými vládními resorty.

Předmětem hodnocení byl technologický facility management datových center a serverových místností. Dotazník obsahoval 152 otázek hodnotící dílčí parametry datových center a serverových místností. Parametry byly rozděleny do následujících sekcí:

I. Kapacita a spolehlivost síťového připojení (parametry 1 – 35)
II. Konektivita k internetu (parametry 36 – 47)
III. Obecné vlastnosti datového centra (parametry 48 – 67)
IV. Lokalita (parametry 87 –107)
V. Generátory a palivové nádrže (parametry 108 – 127)
VI. Procesní zabezpečení (parametry 128 – 152)

Zpracovány byly dotazníky obsahující data o 47 datových centrech a serverových místnostech. Průzkum proběhl v období červenec až říjen 2015. Zpracována byla data, která byla k dispozici nejpozději 1. listopadu 2015.

4. Vyhodnocení výsledků průzkumu

4.1. Obecné zhodnocení

Z vyplněných dat lze vyvodit, že parametry jednotlivých dotazovaných datových center se liší jak svou velikostí a energetickou náročností a z toho plynoucích nákladů na provoz, tak i poskytovanými službami.

Celkový počet provozovaných skříňových rozvaděčů (dále jen Racků) s IT technologiemi se pohybuje v rozmezí 1 – 128 s celkovým příkonem 1 – 558 kW.

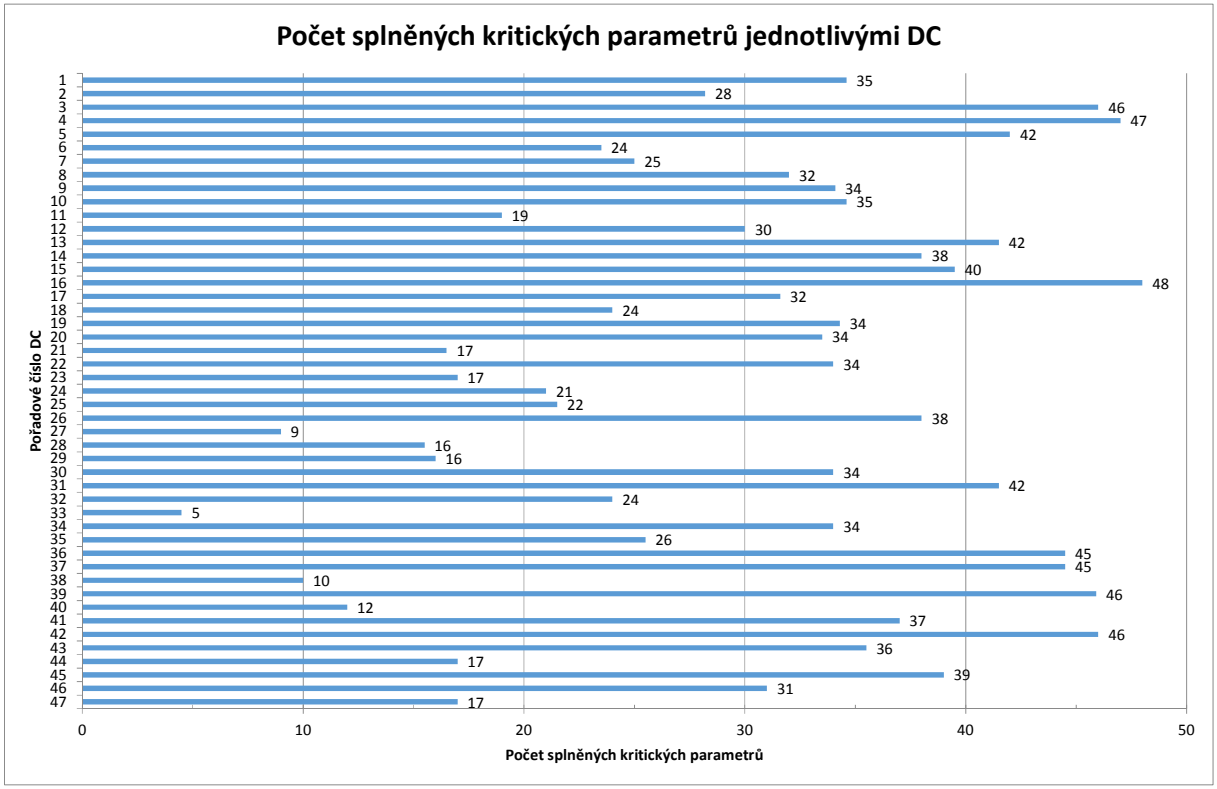
Počet provozovaných Racků s IT technologiemi v interních DC a serverových místnostech je v rozmezí 0 -108 s celkovým příkonem 0 – 358 kW.

Plocha vlastních datových center a serverových místností (dále jen DC) je v rozmezí 0,81 – 642 m^2.

4.1.1. Kritické parametry

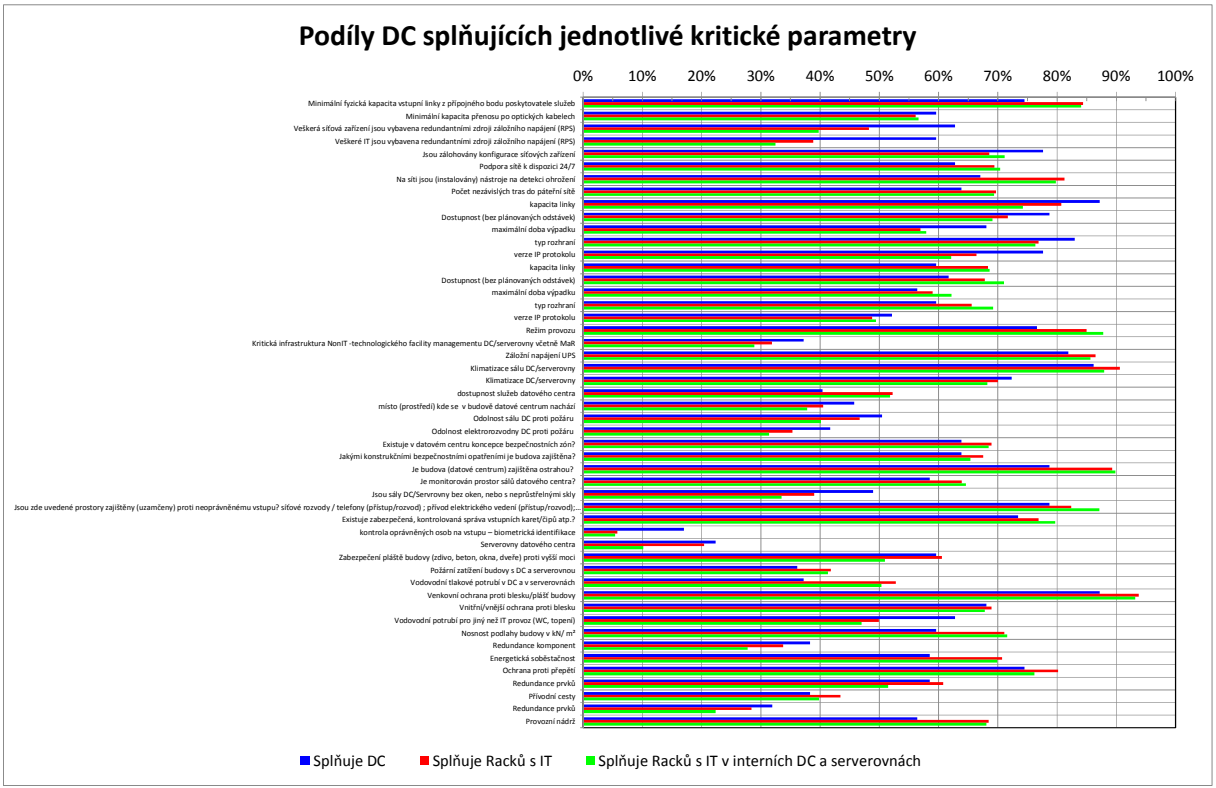
Ze 152 parametrů bylo 50 identifikováno jako kritické.

- Není žádný kritický parametr, který by byl splněn všemi DC, viz Obr. 1.
- Celkem 10 ze 46 hodnocených DC splnilo alespoň 80 % kritických parametrů.



Obr. 1 Počet splněných kritických parametrů

- Žádné DC nesplnilo všechny kritické parametry.
    - Jejich splnění je podmíněno buď investicemi do jednotlivých DC, nebo vybudováním jednoho DC (a jeho klonů) – G-Cloudu.
- V obecné rovině nelze konstatovat, že velká DC splňují více kritických parametrů než menší DC.
- Dle našeho názoru by následující parametry měly být zařazeny mezi kritické
    - parametr 66 – Riziko povodně.



Obr. 2 Podíly DC splňujících jednotlivé kritické parametry

5. Relevantní legislativa

Datová centra a serverové místnosti musí splňovat požadavky s ohledem na platnou legislativu. Klíčová část legislativy byla schválena před necelým rokem v prosinci 2014 a navazuje na krizový zákon č. 240/2000 Sb. o krizovém řízení:

- Nařízení vlády 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury ve smyslu novely 315/2014 Sb.
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, kterou se stanovují „významné“ informační systémy a určující kritéria.
- Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti.

5.1. Zákon 240/2000 Sb. o krizovém řízení (krizový zákon)

Stanoví působnost a pravomoc státních orgánů a orgánů územních samosprávných celků a práva a povinnosti právnických a fyzických osob při přípravě na krizové situace, které nesouvisejí se zajišťováním obrany České republiky před vnějším napadením a při jejich řešení a při ochraně kritické infrastruktury (včetně jejich stanovení) a odpovědnost za porušení těchto povinností

5.2. Nařízení vlády 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury ve smyslu novely 315/2014 Sb.

V návaznosti na krizový zákon vláda stanovuje kritéria pro určení prvku kritické infrastruktury:

Průřezová kritéria:

a) obětí s mezní hodnotou více než 250 mrtvých nebo více než 2 500 osob s následnou hospitalizací po dobu delší než 24 hodin,
b) ekonomického dopadu s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu, nebo
c) dopadu na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125000 osob.

Odvětvová kritéria jsou pro stanovena následující obory:
I. Energetika; II. Vodní hospodářství; III. Potravinářství a zemědělství; IV. Zemědělství; V. Doprava; VI. Komunikační a informační systémy; VII. Finanční trh a měna; VIII. Nouzové služby

a pro také pro obor „IX. Veřejná správa, v následujícím členění“:

A. Veřejné finance
B. Sociální ochrana a zaměstnanost
C. Ostatní státní správa
D. Zpravodajské služby

5.3. Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, kterou se stanovují „významné“ informační systémy a určující kritéria.

Stanovuje významné informační systémy ČR a kritéria pro jejich určení

Určující kritéria
a) Dopadová určující kritéria:

- úplná nebo částečná nefunkčnost informačního systému po dobu delší než 3 pracovní dny způsobená narušením bezpečnosti informací by mohla mít negativní vliv na činnost orgánu veřejné moci;
- ohrožení nebo narušení prvku kritické infrastruktury;
- více než 10 mrtvých nebo 100 zraněných osob;
- významné finanční nebo materiální ztráty orgánu veřejné moci pro taxativně vymezené agendy;
- zásah do osobního života postihující nejméně 50 000 osob.

b) Oblastní určující kritéria – vymezeno ve speciální příloze

V Příloze (č. 1) je vyjmenováno 92 konkrétních „Významných informačních systémů“ ČR.

5.4. Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti

Stanovuje obsah a strukturu bezpečnostní dokumentace pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační

systém, obsah bezpečnostních opatření, rozsah jejich zavedení, typy a kategorie kybernetických bezpečnostních incidentů, náležitosti a způsob hlášení kybernetického bezpečnostního incidentu, náležitosti oznámení o provedení reaktivního opatření a jeho výsledku.

6. Shrnutí a závěr

Předmětem hodnocení byl technologický facility management datových center a serverových místností. Zpracovány byly dotazníky obsahující data o 47 datových centrech a serverových místnostech. Dotazník obsahoval 152 otázek hodnotící jejich dílčí parametry, které byly rozděleny do následujících sekcí:

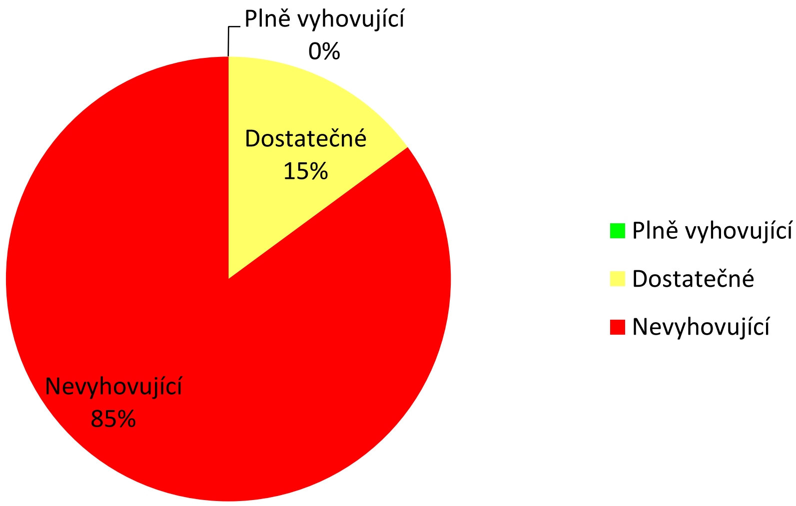
I. Kapacita a spolehlivost síťového připojení
II. Konektivita k internetu
III. Obecné vlastnosti datového centra
IV. Vstupní kontrola
V. Lokalita
VI. Generátory a palivové nádrže
VII. Procesní zabezpečení

Vzhledem k značné nekoherentnosti odpovědí na otázky uvedené sekci Procesní zabezpečení nebyly odpovědi na otázky v této sekci hodnoceny a sekce jako celek nebyla vyhodnocována.

V dotazníku nebyla řešena problematika legislativních požadavků specifikovaných krizovým zákonem (240/2000 Sb.) a navazující legislativa.

K vyhodnocení dotazníků
Dle odpovědí na otázky v každé sekci bylo datové centrum nebo serverová místnost kategorizovány: „splňuje“, „splňuje částečně“, nebo „nesplňuje“.
Při celkovém vyhodnocení:

- jestliže byla alespoň jedna sekce kategorizována „nesplňuje“, tak bylo datové centrum nebo serverová místnost hodnocena jako „nevyhovující“,
- jestliže nebyla žádná sekce kategorizována „nesplňuje“ a zároveň byla alespoň jedna sekce kategorizována „částečně splňuje“, tak bylo datové centrum nebo serverová místnost hodnoceny jako „dostatečné“ s tím, že je nutnost revize datového centra pro získání hodnocení „plně vyhovující“,
- jestliže byly všechny sekce kategorizovány „splňuje“, bylo datové centrum nebo serverová místnost hodnoceny jako „plně vyhovující“.



Z celkového počtu hodnocených datových center a serverových místností bylo hodnoceno:

- 0 % plně vyhovujících,
- 15 % dostatečných,
- 85 % nevyhovujících.

Hodnocení jednotlivých datových center a serverových místností je uvedeno na Obr. 3.

Datové centrum / serverovna	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
Původní označení	1	2			3	4	5	6	7	8	9			10	11	12	13	14	15	16	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33		34	35	36	37	38	39	40			
	a	a	b	c	a	a	a	a	a	a	a	b	c	a	a	a	a																			a	b							a	b	c	d
Kapacita a spolehlivost síťového připojení	✘	✘	!	✔	✔	✘	✘	✘	!	!	✘	✘	✔	✘	!	✔	✘	✘	!	!	✘	✘	✘	✘	✘	!	!	✘	✘	!	✔	!	✘	✘	!	✔	✔	!	✔	!	✘	✔	!	!	!	!	✘
Konektivita k internetu	✔	✔	✔	✔	✘	✘	✘	✘	✔	✔	✘	✘	✘	!	✘	✔	!	✘	✔	✔	✘	✔	✘	!	✘	✔	✘	✘	✘	✘	✘	✔	✘	✘	✔	✔	✔	✘	✔	✘	✘	✔	✔	✔	✔	!	✘
Obecné vlastnosti datového centra	!	!	✔	✔	✔	!	✘	✔	✘	!	!	✔	✔	!	✔	✔	✘	✘	!	!	✘	!	✘	✘	✘	!	✘	✘	✘	!	✔	✘	✘	✔	✘	✔	✔	✘	✔	✘	✔	✔	!	✘	!	✘	!
Vstupní kontrola	!	!	✔	✔	✔	✘	!	!	!	✔	✘	✘	✔	✔	✔	✔	✘	!	!	!	✘	✔	✘	✘	✘	✔	✘	✘	✘	!	✔	✘	✘	✔	✘	!	✔	✘	✔	✘	!	✔	!	✘	!	!	!
Lokalita	✘	✘	!	!	✔	✘	✘	✘	✘	✘	✘	✘	!	!	!	!	✘	✘	✘	✘	✘	!	✘	✘	✘	✘	✘	✘	✘	✘	!	✘	✘	!	✘	!	!	✘	!	✘	✘	!	✘	✘	✘	✘	✘
Generátory a palivové nádrže	!	✘	!	✔	✔	✘	!	!	✘	!	✘	✔	✔	!	✔	✔	!	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✔	✘	✘	!	✘	!	!	✘	✔	✘	!	✔	✘	✘	✘	✘	✘
Celkem	✘	✘	!	!	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	!	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	!	!	✘	!	✘	✘	!	✘	✘	✘	✘	✘

Hodnocení sekcí
✔ Splňuje
! Částečně splňuje
✘ Nesplňuje

Celkové hodnocení
✔ Plně vyhovující
! Dostatečné
✘ Nevyhovující

Obr. 3 Celkové vyhodnocení po sekcích

7. Doporučení

Doporučujeme provést revizi dotazníků od respondentů pro doplnění chybějících odpovědí a verifikaci stávajících a tím případné upravení výsledků.

Doporučujeme zpracování nového dotazníku pokrývajícího následující oblasti:

a) Naplnění legislativních požadavků z hlediska krizového zákona a příp. dalších
b) Nákladový rozbor
c) Nově zpracovat sekci Procesní zabezpečení.
d) Další témata

Ad a) Legislativa

Rozbor problematiky s ohledem na práci s kritickými daty v datových centrech a souladu se zákony o krizovém řízení (240/200 Sb.), nařízením vlády č 432/2010 Sb., vyhláškou č. 317/2014 Sb. a vyhláškou č. 316/2014 Sb. v aktuálních zněních.

Ad b) Nákladový rozbor

Má klíčový význam vzhledem k tomu, že úspory nákladů jsou zásadním argumentem pro koncentraci výpočetní techniky

Investice (možná struktura či variantní otázky):

- Vynaložené investice
- Očekávané investice

Provozní náklady:

- Náklady na provoz
- Náklady na údržbu
- Osobní náklady

Udržitelnost

- Plán investic

Klíčovým problémem nákladového rozboru bude vytvoření vhodné soustavy metrik.

Ad c) Nově zpracovat sekci Procesní zabezpečení

Nově zpracovat sekci Procesní zabezpečení tak, aby byla respondenty jednoznačně chápána.

Ad d) Další témata, která by v rámci dotazníkového průzkumu SPCSS otevřela:

- Životní cyklus používané technologie

- Kritičnost aplikací a případně jejich segmentace
- Potřeby jednotlivých OVM do budoucna
- Ochota konsolidovat infrastrukturu – argumenty pro / proti

8. Pohled ze zahraničí

Vládní organizace i složky centrální vlády v různých částech světa stále častěji využívají sdílené služby formou Cloud Computingu, tedy poskytování služeb, které jsou centralizované a standartizované. Cloud Computing umožní státní správě hospodárnější využití IT investic, a to díky sdílené IT infrastruktuře. Náklady na hardware se vynaloží jen jednou pro centrální uložiště, čímž státní orgány a instituce jako celek optimalizují nasazení a využití IT zdrojů. Další výhodou je zkvalitnění správy IT a urychlení zavádění nových služeb do provozu.

Lze očekávat, že během několika málo let stále více státních organizací v mnoha zemích využije privátního Cloud-u jako dalšího logického kroku navazujícího na virtualizaci datových center a jako prostředku pro dosažení inovací a pružnosti.
V současné době však hlavním důvodem pro budování sdílených center služeb je dosažení vyšší hospodárnosti a snaha snížit náklady snížením investic na hardware. Další výhodou využívání center sdílených služeb je uvolnění tlaku na interní lidské zdroje a snížení externích poplatků za podporu.

Ve světe, v rámci státní správy vnímáme trend využití výhod služeb Cloud-u, nejdále je v této oblasti Velká Británie oproti ostatním zemím Evropské unie. Vlajkovou lodí tzv. G-Cloudu je CloudStore iniciativa. Nicméně i v oblasti střední a východní Evropy se množí příklady využití G-cloudu, či minimálně využití center sdílených služeb. Následující příklady ilustrují snahy jednotlivých vlád využít cloud a centra sdílených služeb.

- Maďarsko zavedlo infrastrukturní Cloud-ová řešení pro ministerstva ve dvou datových centrech.
- Sousedé na Slovensku, konkrétně ministerstva vnitra a financí hodlají implementovat svá datová centra, a tímto ušetřit na nákladech a zároveň zkvalitnit bezpečnost a zvýšit kvalitu poskytovaných služeb.
- Chorvatsko plánuje vytvoření centra sdílených služeb. Pro vybudování centra počítá s financováním y evropských fondů.
- Rumunská vláda zadala projekt konsorciu firem vybudovat Cloud-ovou platformu pro poskytování služeb státním institucím.
- V Polsku ministerstvo financí bude v průběhu příštích čtyř let využívat Cloud-ovou platformu pro řadu e-služeb.

Z uvedených příkladů je zřejmé, že využití Cloud-ových služeb, potažmo centralizace a standartizace správy IT ve státní správě je na vzestupu a je výsledkem racionálních úvah.
Tyto úvahy musí zahrnovat odpovědi na následující otázky:

- Jaké jsou ty hlavní procesní a IT priority, pro které je vhodné řešení využití cloudových služeb
- Jak budou v čase narůstat požadavky na IT zdroje?
- Které procesy, aplikace, oddělení mohou mít užitek ze standardizovaného prostředí, elastického škálování a výhody z rozsahu?