

DEKOMPOZICE ISVS PRO PROVOZ V HYBRIDNÍM PROSTŘEDÍ EGOVERNMENT CLOUDU

Informační systém veřejné správy (dále jen „ISVS“) se definuje jako funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost pro účely výkonu veřejné správy nebo plnění jiných funkcí státu anebo dalších veřejnoprávních korporací¹. Část ISVS, která je jednoznačně oddělitelná od jiných jeho částí a zabezpečuje cílevědomou a systematickou informační činnost, se nazývá komponenta². Jednotlivé komponenty lze nezávisle pořizovat a provozovat samostatně, stejně jako sdílet mezi různými informačními systémy. U moderně navržených ISVS pro provoz v cloudu lze bez značných nákladů nebo dokonce bez přerušení provozu měnit přiřazení komponent aplikace jednotlivým technologickým prvkům, přidávat nebo ubírat komponenty kritické pro odezvu systému.

Způsoby dekomponování a referenční modely moderních informačních systémů³ mají za cíl zvýšit efektivnost využívání prostředků při vývoji a provozování informačních systémů.

Účelem tohoto dokumentu je popsat způsoby dekompozice ISVS s cílem umožnit jejich hybridní provoz s využitím služeb cloud computingu různé bezpečnostní úrovně (dále jen „BÚ“).

Jednotlivé komponenty ISVS mohou být zařazeny do různých BÚ. Důvodem je, že kategorizace celého ISVS do BÚ je realizována na základě analýzy rizik ISVS vzhledem k jeho dostupnosti, důvěrnosti a integritě, a to podle pravidel daných vyhláškou č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci (dále jen „VoBÚ“). Konkrétní ISVS může být zařazen např. do BÚ 4 z důvodu důvěrnosti dat, ale dostupnost a integrita ISVS může být kategorizována do nižších BÚ. Z toho důvodu lze provádět dekompozici a implementovat komponenty ISVS s využitím hybridního eGC.

Hybridní provoz v eGC má dvě základní varianty:

- 1) část (komponenta) ISVS vyžadující nejvyšší bezpečnostní úroveň (tj. BÚ 4) je umístěna ve Státní části eGC (SeGC) a části s nižšími nároky na bezpečnost (tj. BÚ 1 až BÚ 3) v Komerční části eGC (KeGC)⁴,
- 2) jednotlivé části (komponenty) ISVS jsou provozovány pomocí cloudových služeb KeGC s různou BÚ (tj. BÚ 1 – BÚ 3).

¹ Viz § 2, odst. 1, písm. b) zákona č. 365/2000 Sb., o informačních systémech veřejné správy

² Viz § 2, písm. f) vyhlášky č. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy

³ Standardní IS, jako jsou ERP, HR a další) mají mezinárodní IT komunitou vytvořeny referenční modely, které definují vzorovou strukturu a funkčnost jednotlivých komponent IS.

⁴ Následné propojení komponent ISVS, které jsou umístěny v různých provozních prostředích, je vždy a pouze prostřednictvím CMS/KIVS.

Principy dekompozice

Dekompozice a následný hybridní provoz ISVS je možný téměř u každého ISVS. Způsob dekompozice je ale významně závislý na architektuře ISVS, přesněji na tom, zda architektura hybridní provoz umožňuje. Platí ale, že drtivou většinu ISVS lze provozovat hybridně z operačního (provozně funkčního) pohledu.

Způsoby dekompozice

Orgán veřejné správy provádí⁵ dekomponování ve třech nezávislých a vzájemně se kombinujících pohledech, a to:

1. **funkční dělení**, tedy dělení na komponenty podle různých funkcí při podpoře výkonu služeb veřejné správy a provozu orgánu veřejné správy

Prvním pohledem na členění ISVS je dělení na logicky související veřejnosprávní činnosti, které jsou podporovány samostatně funkčními částmi informačního systému. Funkční části ISVS zahrnují komponenty od uživatelského rozhraní aplikace přes aplikační logiku až po komunikaci a ukládání dat (funkční silo). Takovéto funkční komponenty mohou vystupovat jako samostatně fungující informační systémy, podporující výkon podмноžiny veřejnoprávních činností. Funkční komponenty mohou být sdíleny mezi více orgány veřejné správy. K jejich pořízení může dojít celou škálou forem od vývoje na zakázku po pořízení hotového řešení v cloudu formou služby (SaaS).

Příkladem může být dělení na:

- část zajišťující interakci s uživateli ISVS (Front End)
- část zajišťující byznys logiku (funkcionalitu) ISVS
- část, která ukládá a zpřístupňuje data ISVS
- část, která zajišťuje infrastrukturní a aplikační monitoring

Nejvyšší BÚ má obvykle ta část, která ukládá a zpřístupňuje agregovaná data ISVS, protože její zranitelnost vůči hrozbám ztráty důvěrnosti nebo integrity dat lze obvykle považovat za nejvyšší. Ostatní části pak mohou mít nižší BÚ.

2. **technologické dělení**, tedy dělení podle technologických platforem sloužících pro vytvoření, rozvoj a provoz informačních systémů a jejich komponent

Druhým pohledem na členění ISVS je dělení na technologické vrstvy, kde jedna vrstva poskytuje služby pro vrstvu nadřazenou. Uplatněním tohoto konceptu lze dosáhnout vyšší flexibility a nezávislost při změně určitých technologických celků (komponent). Poskládáním technologických komponent na sebe je vytvořena samostatně funkční komponenta informačního systému (funkční silo). Technologické komponenty jsou často sdíleny mezi funkčními komponentami informačních systémů jednoho orgánu. Moderní technologie, jako například virtualizace a cloud, dovolují sdílení i mezi různými typy zákazníků. Mohou být samostatnou sdílenou funkční částí infrastruktury, například tiskové

⁵ Viz § 22 vyhlášky č. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy; účinná od 1. 7. 2024.

řešení, nebo dokonce technologické celky budovy, například strukturovaná kabeláž nebo klimatizace datacentra. Formy pořízení se pohybují od nákupu a instalace fyzického zařízení až po pronájem provozních služeb v cloudu (PaaS, IaaS a SaaS).

Příkladem může být dělení na:

- fyzické a virtuální jádro procesoru
- hypervizor
- operační systém a nad ním platformní služby jako např. adresářové služby (directory) a služby autentizace a autorizace,
- platformní služby (PaaS) a na nich provozovaná SW aplikace (s tím, že provozovatel PaaS a výrobce/provozovatel SW aplikace se mohou lišit).

Pro cloudové služby je typické technologické dělení při výstavbě ISVS s vysokou dostupností, kdy nejnižší vrstvou může být ukládání dat na levné komerční disky (JBOD⁶), jejich spojením s využitím softwarového řešení redundance vznikne úložiště s vyšší odolností, a následně propojením několika takových geograficky oddělených úložišť a další softwarovou vrstvou transakčního řízení může být vytvořen subsystém správy dat s vysokou dostupností a spolehlivostí.

3. **provozní dělení**, tedy dělení na prostředí, podle jejich různého využití v životním cyklu ISVS a jejich komponent.

Třetí pohled na členění ISVS zohledňuje existenci různých provozních prostředí, sloužících definovaným účelům během životního cyklu ISVS. Tyto účely jsou typicky vývoj a předprodukční testování funkcí ISVS, školení uživatelů, testování integrací komponent a informačních systémů, reprodukce a analýza chyb, provoz archivu po ukončení produkčního provozu. Taková prostředí musejí být navržena tak, aby jakákoliv akce v neprodukčním prostředí nevyvolala nežádoucí změny v prostředí produkčním a případné výstupy z neprodukčního prostředí byly nezáměnné s produkčními výstupy

Příkladem může být dělení na:

- Vývojové prostředí
- Testovací prostředí
- Školící prostředí
- Prostředí pro ostrý provoz
- Sekundární Site Recovery instance ISVS resp. „Cold backup“
- Záloha dat

Bývá obvyklé, že nejvyšší BÚ má přiřazeno prostředí pro ostrý provoz ISVS. Ostatní části mohou mít nižší BÚ, pokud jsou provozně oddělitelné a pokud vykazují nižší úroveň dopadů podle VoBÚ.

⁶ Just a Bunch of Disks, viz např. <https://www.techtarget.com/searchstorage/definition/JBOD>