DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

Export z Národní architektury eGovernmentu ČR

Obsah

Dekompozice informačních systémů 3
Dekompozice ISVS pro provoz v hybridním prostředí eGovernment cloudu 4

Dekompozice informačních systémů

Orgán veřejné správy provede a udržuje aktuální dekomponování informačních systémů nebo jejich částí[1)] pro podporu rozhodování o jejich dlouhodobém řízení ve třech nezávislých a vzájemně se kombinujících pohledech, a to:

- funkční dělení, tedy dělení na komponenty, podle různých funkcí při podpoře výkonu služeb veřejné správy a provozu orgánu veřejné správy,
- technologické dělení, tedy dělení podle technologických platforem sloužících pro návrh, vytvoření a provozování informačních systémů a jejich komponent,
- provozní dělení, tedy dělení na prostředí, podle jejich různého využití v životním cyklu informačních systémů a jejich komponent.

Orgán veřejné správy uplatní provedené dekomponování informačních systémů zejména v základních dokumentech dlouhodobého řízení.

Dekomponování při funkčním dělení se provádí na všech vrstvách architektury informačních systémů, konkrétně dělením na aplikační komponenty, technologické komponenty a komunikační komponenty.

Při funkčním dekomponování informačních systémů využije orgán veřejné správy klasifikační systémy podle referenčních modelů architektury informačních systémů, a to aplikační a technologický, vydávané ministerstvem.

Při technologickém dekomponování informačních systémů využije orgán veřejné správy klasifikační systémy podle referenčních modelů architektury informačních systémů, a to architektury řešení a technologický, vydávané ministerstvem.

Dekomponování při provozním dělení na prostředí se provádí podle aktuální potřeby životního cyklu jednotlivých informačních systémů nebo jejich komponent, zejména na prostředí pro

- ověření konceptu,
- prvotní zkoušení platforem nebo dodaného hotového řešení,
- vývoj a testování iterací,
- předvádění a schvalování vývojových iterací,
- testování funkčnosti, kvality, výkonu, spolehlivosti a integrace vývojových iterací před akceptací,
- akceptační, předprodukční a produkční testování,
- školení, studium a procvičování obsluhy,
- kontrolu záloh, nácviky obnovy provozu a provozní archiv,
- ověření ukončení provozu, zamknutý systém a archiv po ukončení provozu,
- produktivní využívání,
- analýzy a ověřování v kopii produktivního prostředí.

Pro plnění potřeb ověřování integrace, školení a vývoje lze vytvářet a integrovat komponenty a prostředí s účelově omezeným chováním. Každé takové prostředí musí být jednoznačně identifikovatelné a pro přístup k dalším prostředím užívat pouze své vlastní unikátní identifikátory. Změny údajů vložené prostřednictvím takového prostředí musí být identifikovatelné a jeho činnost nesmí vést na platnou změnu záznamů v produktivní evidenci agendy.

Při využívání a poskytování služeb prostředí s účelově omezeným chováním správce stanoví pravidla pro

- poskytování údajů službami omezeného prostředí co do množství, struktury a skrývání skutečných údajů, zejména osobních, prostřednictvím pseudonymizace, anonymizace a randomizace,
- provádění nebo simulaci provádění transakcí a změn údajů vyvolaných z prostředí s účelově omezeným chováním, které nesmí být vloženy do produktivních databází a registrů jako platné změny,
- vykonávání nebo simulaci vykonávání operací a interakcí s dalšími integrovanými systémy tak, aby bylo

zřejmé, že se jedná o operace vyvolané činností účelově omezeného prostředí,
- vzájemnou dostupnost rozhraní pro poskytování služeb prostředí s účelově omezeným chováním, prostředí produktivního a dalších integrovaných prostředí pro vlastní a cizí systémy, jejich identifikace a vydávání autentizačních prostředků.

Provozovatel může v rámci stanoveném správcem vytvářet, provozovat a ukončovat provoz prostředí pro plnění různých dílčích úkolů v návaznosti na etapu životního cyklu informačního systému nebo i napříč etapami. Při tom musí zajistit při respektování pravidel určených správcem zejména

- jednoznačnou identifikovatelnost prostředí, jím pořízených a měněných údajů, prováděných transakcí a využívaných služeb,
- přidělování identifikátorů, správu identitních prostředků přidělovaných jednotlivým prostředím,
- ochranu citlivých údajů před nežádoucím vyzrazením, zejména z produktivního prostředí,
- ochranu důvěryhodnosti produktivního prostředí a produktivních údajů.

Opatření podle posledních 2 odstavců mohou být součástí návrhu informačního systému a sloužit i jeho vlastnímu vývoji.

Dekompozice ISVS pro provoz v hybridním prostředí eGovernment cloudu

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 systémů (Standardní IS, jako jsou ERP, HR a další mají mezinárodní IT komunitou vytvořeny referenční modely, které definují vzorovou strukturu a funkčnost jednotlivých komponent IS) mají za cíl zvýšit efektivnost využívání prostředků při vývoji a provozování informačních systémů.

Dekompozice zároveň umožňuje 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)[2)],
2. jednotlivé části (komponenty) ISVS jsou provozovány pomocí cloudových služeb KeGC s různou BÚ (tj. BÚ 1 – BÚ 3).

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 provádí[3] 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 podmnožiny 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:
   1. část zajišťující interakci s uživateli ISVS (Front End)
   2. část zajišťující byznys logiku (funkcionalitu) ISVS
   3. část, která ukládá a zpřístupňuje data ISVS
   4. 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 flexibilitu 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 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:
   1. fyzické a virtuální jádro procesoru
   2. hypervizor
   3. operační systém a nad ním platformní služby jako např. adresářové služby (directory) a služby autentizace a autorizace,-
   4. 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 (JBOD[4]), 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

1. Vývojové prostředí
2. Testovací prostředí
3. Školící prostředí
4. Prostředí pro ostrý provoz
5. Sekundární Site Recovery instance ISVS resp. „Cold backup“
6. 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.

1)

Obdobné dekomponování provede orgán veřejné správy také pro prvky sdílené infrastruktury.

2)

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

3)

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

4)

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