SU-MD-su_333

Zvýšenie dostupnosti ezdravia

dátum
Tento dokument obsahuje x strán

Obsah

1 Základné informácie
1.1 Prehľad
1.2 Dôvod
1.3 Rozsah
1.4 Použité skratky a značky
2 Manažérske zhrnutie
2.1 Motivácia
2.2 Popis aktuálneho stavu
2.2.1 Legislatíva
2.2.2 Architektúra
2.2.3 Prevádzka
2.3 Alternatívne riešenia
2.3.1 Alternatíva A – „Názov"
2.3.2 Alternatíva B – „Názov"
2.4 Popis budúceho stavu
2.4.1 Legislatíva
2.4.2 Architektúra
2.4.3 Prevádzka
2.4.4 Ekonomická analýza

Zoznam tabuliek

Tabuľka 1 Základné informácie - zhrnutie
Tabuľka 2 Skratky a značky
Tabuľka 3 Motivácia – budúci stav
Tabuľka 4 Legislatíva – aktuálny stav
Tabuľka 5 Biznis architektúra - aktuálny stav
Tabuľka 6 Architektúra informačných systémov - aktuálny stav
Tabuľka 7 Technologická architektúra - aktuálny stav

Tabuľka 8 Bezpečnostná architektúra - aktuálny stav
Tabuľka 9 Prevádzka - aktuálny stav
Tabuľka 10 Legislatíva - budúci stav
Tabuľka 11 Biznis architektúra – budúci stav
Tabuľka 12 Architektúra informačných systémov - budúci stav
Tabuľka 13 Technologická architektúra - budúci stav
Tabuľka 14 Implementácia a migrácia
Tabuľka 15 Bezpečnostná architektúra - budúci stav
Tabuľka 16 Prevádzka - budúci stav
Tabuľka 17 Ekonomická analýza - budúci stav

Základné informácie

Prehľad

Kto tvorí štúdiu, ktoré organizácie budú implementovať projekt, identifikácia organizácii v zriaďovateľskej pôsobnosti, identifikácia príslušného úseku verejnej správy, agendy verejnej správy a životnej situácie.
Tabuľka 1 Základné informácie - zhrnutie

Štúdiu uskutočniteľnosti pre Zvýšenie dostupnosti ezdravia (ďalej len ZDE) pripravilo Národné centrum zdravotníckych informácií. Projekt ZDE bude implementovať NCZI, ktoré bude zároveň prijímateľom nenávratného finančného príspevku pre realizáciu projektu.

Projekt bude financovaný z prostriedkov Operačného programu Integrovaná infraštruktúra – Prioritná os 7 Informačná spoločnosť. Projekt bude primárne prispievať k realizácii špecifického cieľa 7.8 Racionalizácia prevádzky informačných systémov pomocou eGovernment cloudu.

eZdravie alebo aj elektronické služby zdravotníctva boli vytvorené za účelom zvýšenia kvality poskytovanej zdravotnej starostlivosti, hlavne prostredníctvom zdieľanej zdravotnej dokumentácie medzi jednotlivými zdravotníckymi pracovníkmi. Služby sú prevádzkované v súlade so zákonom 153/2013 Z.z. v znení neskorších predpisov v národnom zdravotníckom informačnom systém označovanom ako NZIS (isvs_400). Implementácia služieb bola realizovaná projektami ESZ (projekt_27), ESZ RFaRS (projekt_91) a JRÚZ (isvs_7756), pričom JRÚZ poskytuje výhradne služby len registrov a číselníkov ako údajovú základňu pre ESZ a ESZ RFaRS.

Úspešný štart ezdravia od začiatku minulého roka potvrdil, že Národné centrum zdravotníckych informácií dokáže pohnúť dopredu elektronizáciu zdravotníctva na Slovensku. Keďže sa NCZI osvedčilo pri tomto kľúčovom projekte, dostalo od ministerstva zdravotníctva na starosť aj všetky ostatné rozvojové projekty s cieľom zabezpečiť ich realizáciu a následnú prevádzku. Cieľom na najbližšie roky je expanzia ezdravia realizovaná prostredníctvom štúdii a projektov popísaných v to be stave časti architektúra tejto štúdie. Preto je potrebné rozšíriť existujúci cloud

o komunitný zdravotnícky cloud s dôrazom na vysokú bezpečnosť s cieľom v maximálnej možnej miere ochrániť vysoko citlivé zdravotné dáta občanov pred ich únikom a zneužitím. Plánuje sa sem umiestniť každý nový informačný systém, ktorý bude obsahovať údaje o zdravotnom stave osoby. Cieľom tejto štúdie je pripraviť vysoko bezpečné a prevádzkovateľné riešenie, ktoré poskytne služby v rozsahu preferovanej varianty pre nasledujúce oblasti:

- Pre NZIS, aby mohol poskytovať vysoko dostupné a bezpečné existujúce elektronické služby zdravotníctva (eRecept, eVyšetrenie, eLab, eMedikáca, eObjednanie, Pacientsky sumár, NPZ, EZKO, Autentifikáciu ZPr a občana, registre a číselníky)
- Pre nové rozvojové projekty popísané v TO BE stave v časti architektúra s cieľom vytvoriť nákladovo efektívne, bezpečné a vysoko dostupné prostredie pre ich prevádzku

Zároveň sa vybuduje nový architektonický rámec a Enterprise architektúra rezortu zdravotníctva s jasne definovanými pravidlami, ktoré budú musieť splniť novo vznikajúce riešenia, pokiaľ v zmysle zákona 305/2013 budú označené ako informačné systémy verejnej správy,ktoré obsahujú údaje spracúvané na účely poskytovania zdravotnej starostlivosti, alebo obsahujúce údaje o zdravotnom stave osoby na účely výkonu verejného zdravotného poistenia, ktoré budú pracovať s citlivými zdravotnými dátami.

Výsledkom projektu bude:

- Vybudované primárne dátové centrum
- Migrované ezdravie, platformový redizajn na nové architektonické princípy a technológie a migrácia existujúcich služieb NZIS do novej infraštruktúry
- Pripravená infraštruktúra pre nové rozvojové projekty popísané v TO BE stave v časti architektúra

Zdôvodnenie využitia národného projektu a vylúčenia výberu projektu prostredníctvom výzvy

Projekt je navrhnutý ako národný projekt. Celá oblasť problematiky, ktorá je predmetom projektu je vo výlučnej kompetencii Ministerstva zdravotníctva SR a NCZI pričom kompetencie a pôsobnosť NCZI ustanovuje § 12 zákona č.153/2013 Z. z.. a zriaďovateľská listina, ktorá udeľuje NCZI mandát pre informatizáciu a elektronizáciu zdravotníctva.

Cieľovou skupinou sú zainteresované strany v rezorte zdravotníctva, ako napríklad zdravotnícki pracovníci, poskytovatelia zdravotnej starostlivosti, prijímatelia zdravotnej starostlivosti a vybrané inštitúcie v rezorte zdravotníctva, ktoré pracujú so zdravotnými dátami. Rezort zdravotníctva a jeho inštitúcie majú celonárodné pokrytie a zavedenie riešenia pre podporu zvýšenia dostupnosti ezdravia je potrebné riešiť centrálne a na národnej úrovni.

Prijímateľa/partnera národného projektu a dôvod jeho určenia

Prijímateľom projektu je NCZI. NCZI je štátna príspevková organizácia, ktorej zriaďovateľom je Ministerstvo zdravotníctva Slovenskej republiky. Postavenie a úlohy NCZI upravuje zákon č.153/2013 Z. z..

Podrobnejšie kompetencie a pôsobnosť NCZI ustanovuje § 12 zákona č.153/2013 Z. z.. podľa ktorého NCZI okrem iného:

- vykonáva úlohy v oblasti informatizácie zdravotníctva, správy národného zdravotníckeho informačného systému, štandardizácie zdravotníckej informatiky, zdravotníckej štatistiky a poskytovania knižnično-informačných služieb v oblasti lekárskych vied a zdravotníctva
- je správcom a prevádzkovateľom národného zdravotníckeho informačného systému; prevádzku národného zdravotníckeho informačného systému zabezpečuje národné centrum v spolupráci s poskytovateľmi zdravotnej starostlivosti a zdravotnými poisťovňami
- vedie národné zdravotnícke administratívne registre a spravuje národné zdravotné registre
- určuje spôsob identifikácie, autentizácie a autorizácie pri využívaní elektronických služieb zdravotníctva a spôsob používania technických zariadení na to určených
- plní úlohy certifikačnej autority pre používanie elektronického podpisu v zdravotníctve
- poskytuje informácie z národného zdravotníckeho informačného systému
- poskytuje spracúvané údaje z národných zdravotníckych administratívnych registrov, národných zdravotných registrov, zisťovaní udalostí charakterizujúcich zdravotný stav populácie a štatistických výkazov v zdravotníctve
- metodicky usmerňuje poskytovateľov zdravotnej starostlivosti a zdravotné poisťovne v oblasti komunikácie s národným zdravotníckym informačným systémom
- plní úlohy národného kontaktného bodu pre oblasť elektronického zdravotníctva

Partnerom národného projektu bude Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, ktorý je v zmysle ods. § 34a, bodu 1b) Zákona č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy ústredným orgánom štátnej správy pre oblasť informatizácie spoločnosti. V súlade s Operačným programom Integrovaná infraštruktúra 2014 - 2020 si bude ÚPPVII uplatňovať maximálne 3 % oprávnených výdavkov projektu pre implementáciu štandardov riadenia informačno - technologických projektov, ktoré zabezpečia aktívnu participáciu na riadení projektu a komplexné riadenie budovania informačnej spoločnosti. 3% sa budú uplatňované len v rozsahu dodávaných prác a nie z ceny nákupu HW a SW.

Príslušnosť národného projektu k relevantnej časti PO7 OPII	INVESTIČNÁ PRIORITA 2c): Posilnenie aplikácií IKT v rámci elektronickej štátnej správy, elektronického vzdelávania, elektronickej inklúzie, elektronickej kultúry a elektronického zdravotníctva ŠPECIFICKÝ CIEĽ 7.8: Racionalizácia prevádzky informačných systémov pomocou eGovernment cloudu Kód intervencie 48 : IKT - iné druhy infraštruktúry IKT/rozsiahlych počítačových zdrojov/zariadení
Indikatívna výška finančných prostriedkov určených na realizáciu národného projektu	48 109 246 € s DPH

Dôvod

Dôvod vykonania štúdie uskutočniteľnosti. Definovanie IT stratégie a vízie architektúry organizácie verejnej správy.

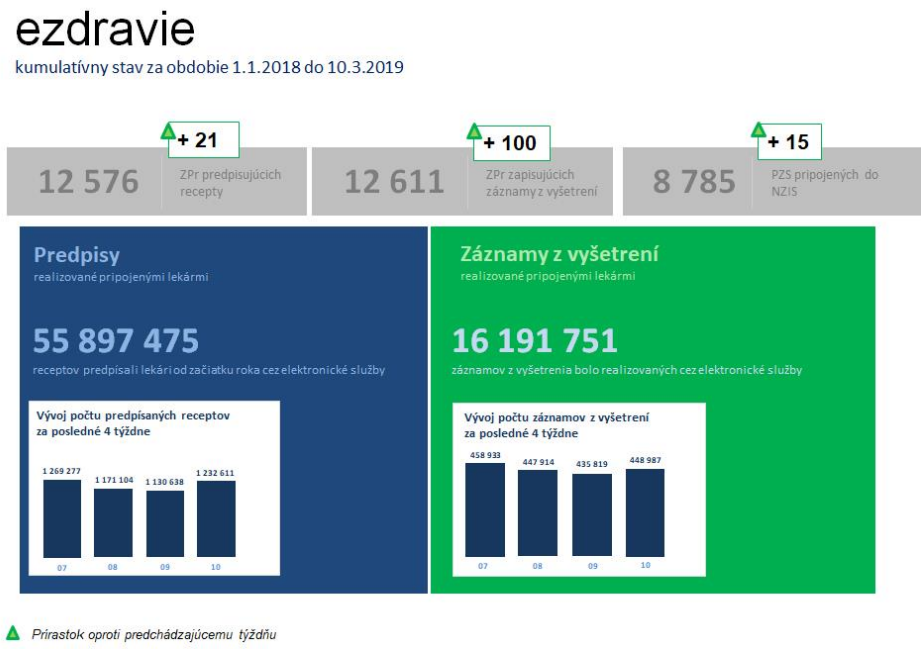
Zdravotná starostlivosť sa dotýka každého z nás. Sme závislí na prístupe ku kvalitnej a v čase dostupnej zdravotnej starostlivosti. Jej poskytovanie je čoraz väčšou výzvou aj kvôli neustále rastúcemu dopytu so súčasným a neustálym zlepšovaním kvality a efektivity. Výber správneho riešenia a jeho implementácia je často komplexná záležitosť a vyžaduje si svoj čas. Každé zdržanie je zároveň premeškanou príležitosťou pri prevencii a záchrane životov. Elektronické služby online formou sú jedným z nástrojov na podporu poskytovania a zlepšovania zdravotnej starostlivosti. Ich potenciál a používanie musíme kontinuálne zlepšovať.

Pre potreby zvýšenia dostupnosti elektronických služieb poskytovaných informačným systémom NZIS pre občanov, zdravotníckych pracovníkov a poskytovateľov zdravotnej starostlivosti a zabezpečenia kontinuálnej zdravotnej starostlivosti je potrebné vytvoriť riešenie , ktoré umožní vyriešiť existujúce problémové oblasti:

- **Zastaraná infraštruktúra** - Ezdravie beží na zastaranej HW a SW infraštruktúre , ktorá bola nakupovaná v rozmedzí rokov 2009 až 2013. Riešenie síce beží vo vysokej dostupnosti na 2 vetvách, avšak výpadok jednotlivých prvkov sa stáva pomerne častou záležitosťou. Rovnako mnohé prvky sú už od výrobcov nepodporované. Preto prevádzka mitiguje na dennej báze riziká spojené s výpadkami. Pre nové projekty je potrebné pripraviť kapacitne a technologicky nové riešenie, ktoré umožní ich nasadenie do prevádzky.
- **Obmedzený dynamicky poskytovaný výkon** – Prevádzka elektronických služieb zdravotníctva poukázala na problém tzv. peakov, kde počas napr. zvýšeného chrípkového obdobia je dopyt po volaní služieb nárazový v podobe zvýšených návštev u lekára a následného zvýšeného počtu predpísaných a vybraných receptov. V praxi to znamená,

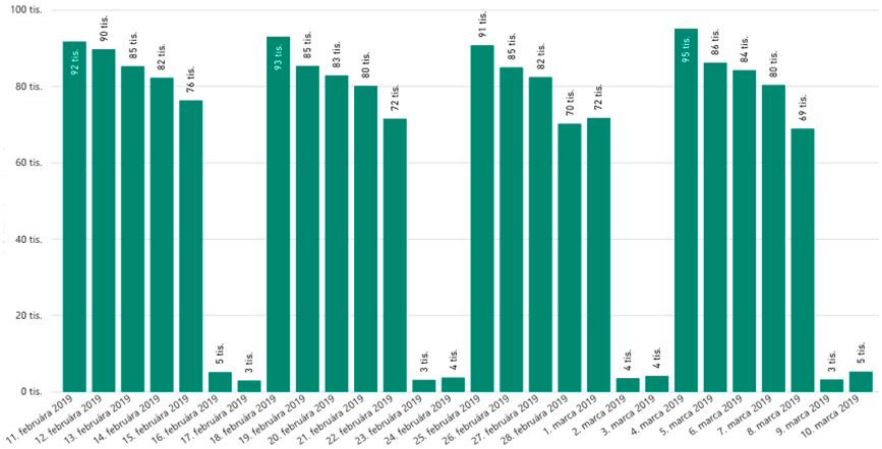
že napr. v ranných hodinách môže narásť výkon až na 5 násobok bežnej prevádzky. Kapacitne bol systém dimenzovaný na bežnú prevádzku s lineárnym rozložením záťaže zvládnuť peak do 300req/s. Aktuálne výkon je postačujúci z dôvodu, že nie všetci PZS sú pripojené, avšak postupne dochádza k zvyšovaniu penetrácie. Napr. iba pre zapísané ambulantné vyšetrenia (recepty je možné násobiť krát 3 pre zápis a výdaj) je stav nasledujúci

Stav pripojenosti k 10.3.2019:



Graf nárastu počtu zápisov za deň k 10.3.2019:

Počet záznamov – odborné vyšetrenie
za obdobie od 11.02.2019 do 10.03.2019



- **Zastaraný dizajn platforiem a problematická migrácia na novšie verzie –** Vzhľadom na udržateľnosť existujúceho riešenia 5 rokov je potrebné po ukončení tohto obdobia vykonať redizajn riešenia na úrovní platforiem a použitých SW a vykonať upgrade na novšie verzie a tak uplatniť modernejšieho technológie v riešení, čo umožní optimalizáciu riešenia s dopadom aj na optimalizáciu prevádzky.
- **Zastarané architektonické princípy –** Riešenie vychádza zo schválenej architektúry na prelome rokov 2010 a 2011. Odvtedy sa posunuli trendy a technológie významne dopredu. Rovnako boli stanovené nové architektonické, bezpečnostné a iné princípy v zmysle NKIVS a nových zákonov o KB a GDPR, ktoré existujúce riešenie reflektuje len čiastočne.
- **Chýbajúci disaster recovery** – Riešenie nemá záložné DC, čo pre takýto systém pre prácu s tak citlivými dátami a potrebnými dátami pre rozhodovanie lekára je absolútna nutnosť. Lekári už dnes netlačia recepty a v prípade, že by došlo najhoršiemu scenáru výpadku primárneho DC je obnova časovo skôr ako do mesiaca nemožná v prípade, že by bola dostupná okamžitá vyhovujúca infraštruktúra v inom DC. Tento problém zohľadňuje štúdia v maximalistickej variante.
- **Riziko kompromitácie ezdravia** – v kontexte ostatných problémov sa zvyšuje riziko, že dôjde k bezpečnostnému incidentu, ktorý by kompromitoval samotné riešenie. Dopad z neho vyplývajúci by mohol spochybniť bezpečnosť riešenia ako takého.
- **Zastaraný monitoring bezpečnostných incidentov** – ako východisko je vnímanie problému č.4, kde aj bezpečnosť musí prejsť revíziou a novým vyhodnotením modelu hrozieb a aplikovaním nových opatrení tak aby sa reflektovali najnovšie modely hrozieb. Následne je potrebné aplikovať nové prevádzkové procesy do praxe a nastaviť nový monitoring. Existujúce riešenie neumožňuje integráciu s pripravovanými riešenia na úrovni eGOV.
- **Zastaraný monitoring prevádzkových incidentov** – ako východisko je vnímanie problému č.4, kde aj prevádzka musí prejsť revíziou a novým vyhodnotením prevádzkového modelu a aplikovaním nových opatrení tak aby sa reflektovali najnovšie

modely pre prevádzku nového riešenia. Následne je potrebné aplikovať nové prevádzkové procesy do praxe a nastaviť nový monitoring.

- **Dlho trvajúci release manažment** - na centrálnych komponentoch zmenu nevieme nasadiť v najideálnejšom prípade do 4 hodín, ale trvá to v niektorých prípadoch aj niekoľko dní. V prípade že ide o nasadenie kritických zmien, tak je to problém a má to dopad na poskytované SLA služby. Preto dnes sme na úrovni dostupnosti služieb niekde okolo 95% a potrebujeme sa dostať na úroveň aby kritické chyby a zmeny boli nasadené s otestovaním max do 24 hodín a tento čas postupne približovať k 4 hodinám. Zdôvodnením dlho trvajúceho release manažmentu je nasledovný problém:
- **Chýbajúci automatizovaný devops a heterogenita prostredí** - Pre každé prostredie je dedikovaný release management, z dôvodu že ostatné prostredia okrem produkčného sú značne oklieštené z finančných dôvodov. Takto nastavené riešenie si vyžaduje značné zdroje na prevádzku ale aj SLA. Heterogenita vedie k chybám, kde sa častou opravuje dodaný balíček a tak predlžuje čas.

Projekt je plánovaný v súlade s nasledovnými dokumentami:

- Stratégia EÚ v oblasti zdravia **„Spoločne za zdravie“** je v plnej miere v súlade so všeobecnými cieľmi stratégie Európa 2020. Európa 2020 sa zameriava na transformáciu hospodárstva EÚ na inteligentnú, udržateľnú a inkluzívnu ekonomiku pre všetkých, ktorá nie je možná bez zdravého obyvateľstva.
- EU stratégiou schválila vláda SR tzv. **Strategický rámec v oblasti starostlivosti o zdravie pre roky 2014 až 2030**.
- Informácie a dáta v zdravotníctve, najmä zdravotné záznamy, ktoré sú zaradené v zmysle nariadenia Európskeho parlamentu **o GDPR (679/2016 článok 9) do osobitnej kategórie osobných údajov**, majú požiadavku aj na zvýšené technické a technologické zabezpečenie proti možným únikom a zneužitiu treťou osobou alebo stranou.
- **Zákon o e-Governmente č. 305/2013 Z.z. podľa paragrafu 2 odsek 2 písmeno d)** vymedzil mimo pôsobnosť tohto zákona tie informačné systémy, ktoré obsahujú údaje spracúvané na účely poskytovania zdravotnej starostlivosti a na informačné systémy obsahujúce údaje o zdravotnom stave osoby na účely výkonu verejného zdravotného poistenia.
- Stratégia informatizácie verejnej správy SR - Štátna správa bude používať dostatočne robustnú integrovanú komunikačnú a údajovú infraštruktúru pre poskytovanie elektronických služieb a svoju vnútornú komunikáciu
- Národná koncepciou informatizácie verejnej správy SR – Strategická priorita: Vládny cloud a naplnenie princípov.
- Strategický dokument pre oblasť rastu digitálnych služieb a oblasť infraštruktúry prístupovej siete novej generácie (2014 – 2020) – rozvoj elektronických služieb, využívanie otvorených údajov a podpora procesov efektívnej verejnej správy
- Operačný programom Integrovaná infraštruktúra, Prioritná os 7 – špecifický cieľ 7.8: Racionalizácia prevádzky informačných systémov pomocou eGovernment cloudu
- Platná legislatíva popísaná v štúdii

- **Reformný zámer** – riešenie je v súlade so schváleným Reformným zámerom e-Zdravie: Zabezpečenie dostupnosti a rozšírenie služieb elektronického zdravotníctva, kde sa v ďalších opatreniach uvádza, že bude:
    - Pripravovaný DC projekt (v spolupráci s MF SR a Úradom podpredsedu vlády) - Existujúci systém NZIS je prevádzkovaný v jednej lokalite na infraštruktúre, ktorá bola nakupovaná priebežne a morálne a technologicky zastaráva. Preto je potrebné vykonať nasledovné aktivity, ktoré umožnia infraštruktúru:
        - Zabezpečiť stabilnú prevádzku a podporu 24/7 pre existujúcu infraštruktúru s cieľom dosiahnuť škálovateľný výkon pre plný rollout pre existujúce služby eso1/1+
        - Zabezpečiť rozšírenie infraštruktúry pre prevádzku nových plánovaných služieb eso2, pre nasadenie hubu pre konsolidáciu dát atď.
        - Vybudovať záložné riešenie v sekundárnej lokalite
        - Predpokladom je riešenie architektonicky navrhnúť tak, aby bolo cloud ready pre vybudovanie privátneho rezortného cloudu Ministerstva zdravotníctva

    - Bezpečnosť údajov

Aktuálna infraštruktúra, na ktorej je prevádzkovaný systém NZIS morálne zastaráva a niektoré infraštruktúrne komponenty majú viac ako 10 rokov a hrozí kedykoľvek riziko, že môžu vypadnúť také kritické prvky, ktoré môžu narušiť kontinuálne poskytovanie elektronických služieb pre zabezpečenie zdravotnej starostlivosti občanom. Ďalej vyššie spomenuté dôvody a vplyv nových schválených dokumentov a zákonov majú významný dopad na existujúce riešenie. Je žiaduce riešiť tento národný projekt v zmysle vyššie uvedených bodov schváleného RZ a tak umožniť prevádzku informačných systémov v rezorte zdravotníctva v prostredí bez znížených bezpečnostných požiadaviek na aktuálne fungujúce a prípadne plánované informačné systémy rezortu zdravotníctva.

Rozsah

Rozsah oblastí, v ktorom sa štúdia venuje projektu, do akej hĺbky sa venuje jednotlivým oblastiam.

Štúdia uskutočniteľnosti vychádza z metodického usmernenia pre spracovanie štúdií uskutočniteľností v rámci Operačného programu Integrovaná infraštruktúra ako aj referenčného architektonického rámca verejnej správy a nadväzuje na „Architektonickú víziu verejnej správy" . Štúdia bola počas prípravy dopĺňaná a upravovaná v zmysle požiadaviek a odporúčaní Úradu podpredsedu vlády SR pre investície a informatizáciu, Útvaru hodnoty za peniaze MFSR a pripomienok a odporúčaní zástupcov odbornej verejnosti. Rozsah doplnení a príloh presahuje rámec údajov požadovaných aktuálne platnou riadiacou dokumentáciou, pričom sa snaží okrem

reakcií na pripomienky uvádzať aj vysvetlenia k jednotlivým princípom aktuálnej NKIVS, ktoré nie sú s ohľadom na špecifiká uplatniteľné pre NCZI.

eZdravie alebo aj elektronické služby zdravotníctva boli vytvorené za účelom zvýšenia kvality poskytovanej zdravotnej starostlivosti, hlavne prostredníctvom zdieľanej zdravotnej dokumentácie medzi jednotlivými zdravotníckymi pracovníkmi. Služby sú prevádzkované v súlade so zákonom 153/2013 Z.z. v znení neskorších predpisov v národnom zdravotníckom informačnom systém označovanom ako NZIS (isvs_400). Implementácia služieb bola realizovaná projektami ESZ (projekt_27), ESZ RFaRS (projekt_91) a JRÚZ (isvs_7756), pričom JRÚZ poskytuje výhradne služby len registrov a číselníkov ako údajovú základňu pre ESZ a ESZ RFaRS.

Úspešný štart ezdravia od začiatku minulého roka potvrdil, že Národné centrum zdravotníckych informácií dokáže pohnúť dopredu elektronizáciu zdravotníctva na Slovensku. Keďže sa NCZI osvedčilo pri tomto kľúčovom projekte, dostalo od ministerstva zdravotníctva na starosť aj všetky ostatné rozvojové projekty s cieľom zabezpečiť ich realizáciu a následnú prevádzku. Cieľom na najbližšie roky je expanzia ezdravia realizovaná prostredníctvom štúdii a projektov popísaných v to be stave časti architektúra tejto štúdie. Preto je potrebné rozšíriť existujúci cloud o komunitný zdravotnícky cloud s dôrazom na vysokú bezpečnosť s cieľom v maximálnej možnej miere ochrániť vysoko citlivé zdravotné dáta občanov pred ich únikom a zneužitím. Plánuje sa sem umiestniť každý nový informačný systém, ktorý bude obsahovať údaje o zdravotnom stave osoby. Cieľom tejto štúdie je pripraviť vysoko bezpečné a prevádzkovateľné riešenie, ktoré poskytne služby v rozsahu preferovanej varianty pre nasledujúce oblasti:

- Pre NZIS, aby mohol poskytovať vysoko dostupné a bezpečné existujúce elektronické služby zdravotníctva (eRecept, eVyšetrenie, eLab, eMedikáca, eObjednanie, Pacientsky sumár, NPZ, EZKO, Autentifikáciu ZPr a občana, registre a číselníky)
- Pre nové rozvojové projekty popísané v TO BE stave v časti architektúra s cieľom vytvoriť nákladovo efektívne, bezpečné a vysoko dostupné prostredie pre ich prevádzku

Zároveň sa vybuduje nový architektonický rámec a Enterprise architektúra rezortu zdravotníctva s jasne definovanými pravidlami, ktoré budú musieť splniť novo vznikajúce riešenia, pokiaľ v zmysle zákona 305/2013 budú označené ako informačné systémy verejnej správy,ktoré obsahujú údaje spracúvané na účely poskytovania zdravotnej starostlivosti, alebo obsahujúce údaje o zdravotnom stave osoby na účely výkonu verejného zdravotného poistenia, ktoré budú pracovať s citlivými zdravotnými dátami.

Výsledkom projektu bude:

- Vybudované primárne dátové centrum
- Migrované ezdravie, platformový redizajn na nové architektonické princípy a technológie a migrácia existujúcich služieb NZIS do novej infraštruktúry
- Pripravená infraštruktúra pre nové rozvojové projekty popísané v TO BE stave v časti architektúra.

Predkladaný dokument popisuje:

- Legislatívne prostredie, do ktorého bude zasadená implementácia ZDE
- Návrh architektúry riešenia, ktorý nadväzuje na strategickú architektúru verejnej správy, ktorá definuje kľúčové stavebné prvky informačného prostredia verejnej správy a ktorý vychádza z architektonických rámcov budovania verejnej správy (TOGAF® a ArchiMate®)
- Motivácia určuje KPI, základné zainteresované strany a ich záujmy a ciele
- Biznis architektúra definuje biznis procesy, funkcie a služby
- Architektúra informačných systémov znázorňuje kompozíciu systémov a integračné väzby s okolím
- Bezpečnostná architektúra definuje bezpečnostné požiadavky na riešenie
- V časti implementácia a migrácia sú vysvetlené základné etapy projektu
- Prevádzka riešenia popisuje, akým spôsobom bude zabezpečená podpora užívateľov a neustála inovácia podporných a administratívnych procesov
- V časti Ekonomická analýza sú kvantifikované prínosy a náklady, ktoré si implementácia ZDE vyžaduje. V rámci tejto časti sú špecifikované indikatívne náklady pre realizáciu riešenia

Pre každú z vyššie uvedených oblasti riešenia sú identifikované kritéria kvality, na základe ktorých je možné posudzovať návrhy a alternatívne riešenia. Obdobne sú identifikované riziká, ktoré bude potrebné v nasledujúcom období počas prípravy a realizácie projektov eliminovať.

Použité skratky a značky

Tabuľka 2 Skratky a značky

Skratka / Značka	Vysvetlenie
Aplikácia	Softvér, ktorý používa inštanciu služby prostredníctvom väzby služby.
BCM	Business Continuity Management – manažment kontinuity činností
CLI	Command Line Interface - Príkazový riadok
Cloud Natívne Aplikácie (CNA)	Sú aplikácie, ktoré sú špeciálne navrhnuté a vyvíjané pre nasadenie a beh v cloude. Základné princípy, ktoré je potrebné dodržiavať pri CNA sú 12 faktorová aplikácia, devops, CI/CD, mikroslužby a kontajnery. CNA zvyčajne závisia od služieb, ako sú napríklad databázy alebo služby poskytovateľov SaaS tretích strán.
Cloud-native	Prístup k vytváraniu a spúšťaniu aplikácií, ktoré plne využívajú výhody modelu poskytovania cloud computingu. Cloud-native je prístupe, kde je dôležité ako sa vytvárajú a nasadzujú aplikácie, ale nie kde sú nasadzované.
DC	Dátové centrum
DevOps	Alebo aj automatizovaný devops ako súbor procesov medzi vývojom a prevádzkou, skratka z developer operations. Vysvetlenie detail viď https://en.wikipedia.org/wiki/DevOps

DOH	Doplnkové ordinačné hodiny
DPH	Daň z pridanej hodnoty
DRP	Disaster Recovery Plan - Plán obnovy
eAlokácie	Modul ezdravie - Predstavuje skupinu služieb, ktoré umožnia občanom elektronické objednávanie sa k vybranému poskytovateľovi primárnej či špecializovanej zdravotnej starostlivosti, ako aj elektronické objednávanie laboratórnych vyšetrení, očkovania a ďalších zdravotných výkonov.
eID	Elektronický občiansky preukaz
ePZP	Elektronický preukaz zdravotníckeho pracovníka
ESB	Enterprise service bus - integrčno-komunikačný kanál, ktorý sprostredkúva komunikáciu medzi službami prostredníctvom správ
ESZ	Elektronické služby zdravotníctva
EÚ	Európska únia
ezdravie	Programové označenie Národného zdravotníckeho informačného systému
EZK/EZKO	Elektornická zdravotná knižka občana
HW	Hardware
IaaS	Infraštruktúra ako služba
IKT	Informačno-komunikačné technológie
Inštancia služby (Service instantion)	Inštancia služby z ponuky
IS	Informačný systém
JRÚZ	Jednotná referenčná údajová základňa pre ezdravie
KPI	Key Performance Indicator - Kľúčové ukazovatele výkonnosti
Manažované služby (Managed Services)	Sú definované ako služby integrovateľné s PaaS platformou pomocou rozhraní API a umožňujú koncovým používateľom poskytovať na požiadanie rezervované zdroje a poverenia (credentials)
MPD	Medikácia, preskripcia, dispenzácia - modul ezdravie
MR	Magnetická rezonancia
MZ SR	Ministerstvo zdravotníctva SR
NCZI	Národné centrum zdravotníckych informácií
NIS	Nemocničný informačný systém
NOC	Network operations center
NPZ	Národný portál zdravia
NZIS	Národný zdravotnícky informačný systém
OPII	Operačný program integrovaná infraštruktúra
PaaS	Platforma ako služba
Platforma (Platform)	Softvér, ktorý spravuje prostredie cloudu, do ktorého sú nasadzované a prevádzkované aplikácie (CNA) a sprostredkovateľov služieb SB (service brokers).
PREPROD	Pred-produkčné prostredie NZIS

PROD	Produkčné prostredie NZIS
PZS	Poskytovateľ zdravotnej starostlivosti
RČ	Rodné číslo
RTG	Röntgen
RZ	Reformný zámer
SDL	Security development lifecycle
SLA	Service-level agreement - Dohoda o úrovni poskytovaných služieb
Služba PaaS (Service)	Spravovaná ponuka softvéru, ktorý môže byť využitý aplikáciou. Zvyčajne služby vystavujú API, ktoré môžu byť vyvolané na vykonanie nejakej akcie. Existujú aj neinteraktívne služby, ktoré môžu vykonávať požadované akcie bez priameho dotazu z aplikácie
SOC	Security operations center
Sprostredkovateľ služby (SB) (Service Broker)	Servisní sprostredkovatelia riadia životný cyklus služieb. Platformy spolupracujú s SB pri poskytovaní a spravovaní servisných inštancií a servisných väzieb (Binding)
SR	Slovenská republika
SW	Software
UI	User interface - používateľské rozhranie
ÚPVII	Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu
Väzba služby (Service Binding)	Reprezentácia asociácie medzi aplikáciou a inštanciou služby. Väzby služby často obsahujú poverenia (credentials), ktoré aplikácia použije na komunikáciu so inštanciou služby
VC	Vládny cloud
VÚC	Vyšší územný celok
ZDE	Zvýšenie dostupnosti eZdravia
ZP	Zdravotná poisťovňa
ZPr	Zdravotnícky pracovník

Manažérske zhrnutie

Základné zhrnutie. Max 2400 znakov.
Priestor pre sumárny obrázok, nepovinná informácia: ArchiMate štandardný viewpoint – „Introductory viewpoint"

eZdravie alebo aj elektronické služby zdravotníctva boli vytvorené za účelom zvýšenia kvality poskytovanej zdravotnej starostlivosti, hlavne prostredníctvom zdieľanej zdravotnej dokumentácie medzi jednotlivými zdravotníckymi pracovníkmi. Služby sú prevádzkované v súlade so zákonom 153/2013 Z.z. v znení neskorších predpisov v národnom zdravotníckom informačnom systém označovanom ako NZIS (isvs_400). Implementácia služieb bola realizovaná projektami ESZ (projekt_27), ESZ RFaRS (projekt_91) a JRÚZ (isvs_7756), pričom

JRÚZ poskytuje výhradne služby len registrov a číselníkov ako údajovú základňu pre ESZ a ESZ RFaRS.

Úspešný štart ezdravia od začiatku minulého roka potvrdil, že Národné centrum zdravotníckych informácií dokáže pohnúť dopredu elektronizáciu zdravotníctva na Slovensku. Keďže sa NCZI osvedčilo pri tomto kľúčovom projekte, dostalo od ministerstva zdravotníctva na starosť aj všetky ostatné rozvojové projekty s cieľom zabezpečiť ich realizáciu a následnú prevádzku. Cieľom na najbližšie roky je expanzia ezdravia realizovaná prostredníctvom štúdii a projektov popísaných v to be stave časti architektúra tejto štúdie. Preto je potrebné rozšíriť existujúci cloud o komunitný zdravotnícky cloud s dôrazom na vysokú bezpečnosť s cieľom v maximálnej možnej miere ochrániť vysoko citlivé zdravotné dáta občanov pred ich únikom a zneužitím. Plánuje sa sem umiestniť každý nový informačný systém, ktorý bude obsahovať údaje o zdravotnom stave osoby. Hlavným motivátorom národného projektu „Zvýšenie dostupnosti eZdravia“ je naplnenie cieľov a to pripraviť vysoko bezpečné a prevádzkovateľné riešenie, ktoré poskytne služby v rozsahu preferovanej varianty pre nasledujúce oblasti:

- Pre NZIS, aby mohol poskytovať vysoko dostupné a bezpečné existujúce elektronické služby zdravotníctva (eRecept, eVyšetrenie, eLab, eMedikáca, eObjednanie, Pacientsky sumár, NPZ, EZKO, Autentifikáciu ZPr a občana, registre a číselníky)
- Pre nové rozvojové projekty popísané v TO BE stave v časti architektúra s cieľom vytvoriť nákladovo efektívne, bezpečné a vysoko dostupné prostredie pre ich prevádzku

Zároveň sa vybuduje nový architektonický rámec a Enterprise architektúra rezortu zdravotníctva s jasne definovanými pravidlami, ktoré budú musieť splniť novo vznikajúce riešenia, pokiaľ v zmysle zákona 305/2013 Z. z. budú označené ako informačné systémy verejnej správy,ktoré obsahujú údaje spracúvané na účely poskytovania zdravotnej starostlivosti, alebo obsahujúce údaje o zdravotnom stave osoby na účely výkonu verejného zdravotného poistenia, ktoré budú pracovať s citlivými zdravotnými dátami.

Výsledkom projektu bude:

- Vybudované primárne dátové centrum
- Migrované ezdravie, platformový redizajn na nové architektonické princípy a technológie a migrácia existujúcich služieb NZIS do novej infraštruktúry
- Pripravená infraštruktúra pre nové rozvojové projekty popísané v TO BE stave v časti architektúra.

Splnením týchto cieľov sa významne podporí rozvoj eZdravie. Jednou zo základných požiadaviek eZdravie je centralizácia a elektronizácia procesov, nastolenie nových progresívnych platforiem, unifikovanie postupov s cieľom zvýšenia efektívnosti poskytovanej zdravotnej starostlivosti.

Cieľom je aj redizajn existujúceho IS ezdravie podľa novo stanovených princípov a jeho nasadenie do prevádzky podľa preferovanej varianty.

Definované ciele sú východiskom pre ďalší rozvoj ezdravie a ich maximálnym naplnením bude dosiahnutá úroveň architektúry a jej princípov v maximálne možnej miere. Túto mieru budú môcť dosiahnuť aj iné riešenia v rezorte zdravotníctva, avšak budú si môcť voliť aj kombináciu medzi minimalistickou a preferovanou verziou vyskladania služieb.

Bude podporené:

- nariadenie o GDPR, kde informácie a dáta v zdravotníctve, najmä zdravotné záznamy, ktoré sú zaradené v zmysle nariadenia Európskeho parlamentu o GDPR (679/2016 článok 9) do osobitnej kategórie osobných údajov, majú požiadavku aj na zvýšené technické a technologické zabezpečenie proti možným únikom a zneužitiu treťou osobou alebo stranou.
- zákon o e-Governmente č. 305/2013 Z.z. podľa paragrafu 2 odsek 2 písmeno d), prostredníctvom ktorého vymedzil mimo pôsobnosť tohto zákona tie informačné systémy, ktoré obsahujú údaje spracúvané na účely poskytovania zdravotnej starostlivosti a na informačné systémy obsahujúce údaje o zdravotnom stave osoby na účely výkonu verejného zdravotného poistenia.
- bezpečná prevádzka a zvýšená ochrana nových a rozvíjaných/budovaných/migrovaných systémov ako aj obsahu dát chránenej povahy v súlade s uplatnenými výnimkami

Pre informačné systémy, ktoré obsahujú citlivé zdravotné dáta a podľa zákona 305/2013 Z.z. sa na nich vzťahuje výnimka na prevádzkovanie vo vládnom cloude, sa vytvorí sa rezortná infraštruktúra zdravotníctva, ktorá bude predstavovať nové riešenie, ktoré umožní vytvoriť špecifické zóny, ktoré budú spĺňať všetky bezpečnostné požiadavky pre uchovávanie a výmenu dát nielen v rezorte zdravotníctva ale aj mimo neho. Týmto bude podporené aj naplnenie špecifického cieľa 7.8 operačného programu Integrovaná infraštruktúra - Racionalizácia prevádzky informačných systémov pomocou eGovernment cloudu a zároveň bude podporené aj uplatňovanie technických princípov uvedených v Národnej koncepcii informatizácie verejnej správy (NIKVS).

Vyššie uvedený zámer je v súlade so schváleným Reformným zámerom eZdravie: Zabezpečenie dostupnosti a rozšírenie služieb elektronického zdravotníctva, kde sa v ďalších opatreniach uvádza, že bude:

Pripravovaný DC projekt (v spolupráci s MF SR a Úradom podpredsedu vlády) - Existujúci NZIS (ezdravie) je prevádzkovaný v jednej lokalite na infraštruktúre, ktorá bola nakupovaná priebežne a morálne a technologicky zastaráva. Preto je potrebné vykonať nasledovné aktivity, ktoré umožnia infraštruktúru:

- Zabezpečiť stabilnú prevádzku a podporu 24/7 pre existujúcu infraštruktúru s cieľom dosiahnuť škálovateľný výkon pre plný rollout pre existujúce služby eso1/1+
- Zabezpečiť rozšírenie infraštruktúry pre prevádzku nových plánovaných služieb eso2, pre nasadenie hubu pre konsolidáciu dát atď.
- Vybudovať záložné riešenie v sekundárnej lokalite

- Predpokladom je riešenie architektonicky navrhnúť tak, aby bolo cloud ready pre vybudovanie privátneho rezortného cloudu Ministerstva zdravotníctva

Aktuálna infraštruktúra, na ktorej je prevádzkovaný systém ezdravie morálne zastaráva a niektoré infraštruktúrne komponenty majú viac ako 10 rokov a hrozí kedykoľvek riziko, že môžu vypadnúť také kritické prvky, ktoré môžu narušiť kontinuálne poskytovanie elektronických služieb pre zabezpečenie zdravotnej starostlivosti občanom. Ďalej vyššie spomenuté dôvody a vplyv nových schválených dokumentov a zákonov majú významný dopad na existujúce riešenie. Je žiaduce riešiť tento národný projekt v zmysle vyššie uvedených bodov schváleného RZ a tak umožniť prevádzku informačných systémov v rezorte zdravotníctva v prostredí bez znížených bezpečnostných požiadaviek na aktuálne fungujúce a prípadne plánované informačné systémy rezortu zdravotníctva.

Motivácia

Tabuľka 3 Motivácia – budúci stav

Súhrnný popis

Ciele, výstupy a zdôvodnenie je uvedené v predošlých kapitolách. V motivácii sa popisujú rozpad cieľov až na úroveň merateľných KPI.

Jednotlivé zainteresované subjekty a ich rozsah v kontexte riešených problémov:

Subjekt	**Početnosť k 30.10.2018**
Poskytovatelia zdravotnej starostlivosti (PZS)	13 436
NCZI	1

Ciele jednotlivých subjektov

Subjekt	**Cieľ**
NCZI	Prevádzkovo stabilná, bezpečná a cenovo udržateľná infraštruktúra
	Aktualizácia platforiem a zavedenie pay-per-use tam kde to bude možné
	Nastavenie nových architektonických princípov v zmysle moderných trendov
	BCM a DRP v súlade s legislatívnymi požiadavkami
	Zachovanie bezpečnostných požiadaviek minimálne v adekvátnej úrovni k súčasnému stavu a ich posilnenie v súlade s rozšírením o nové modernejšie technológie
	Zavedenie modernizovaného systému monitorovania a vyhodnocovania bezpečnostných incidentov v súlade s novými architektonickými princípmi. Zároveň sa integrovať na centrálny CSIRT
	Zavedenie modernizovaného systému monitorovania a vyhodnocovania prevádzkových incidentov s súlade s novými architektonickými princípmi.
	Zjednodušenie, sprehľadnenie a zrýchlenie zložitých prevádzkových postupov
	Zjednodušenie, sprehľadnenie a zrýchlenie komplikovaného release managementu
	Dynamicky poskytovaný výkon
Poskytovatelia zdravotnej starostlivosti	Stabilné a dostupné elektronické služby zdravotníctva, minimalizácia ich neplánovanej nedostupnosti, tak aby neboli vynucované náklady na administratívu, papier a časové zdržanie ZPr počas výkonu poskytovania zdravotnej starostlivosti.

BCM a DRP v súlade s legislatívnymi požiadavkami

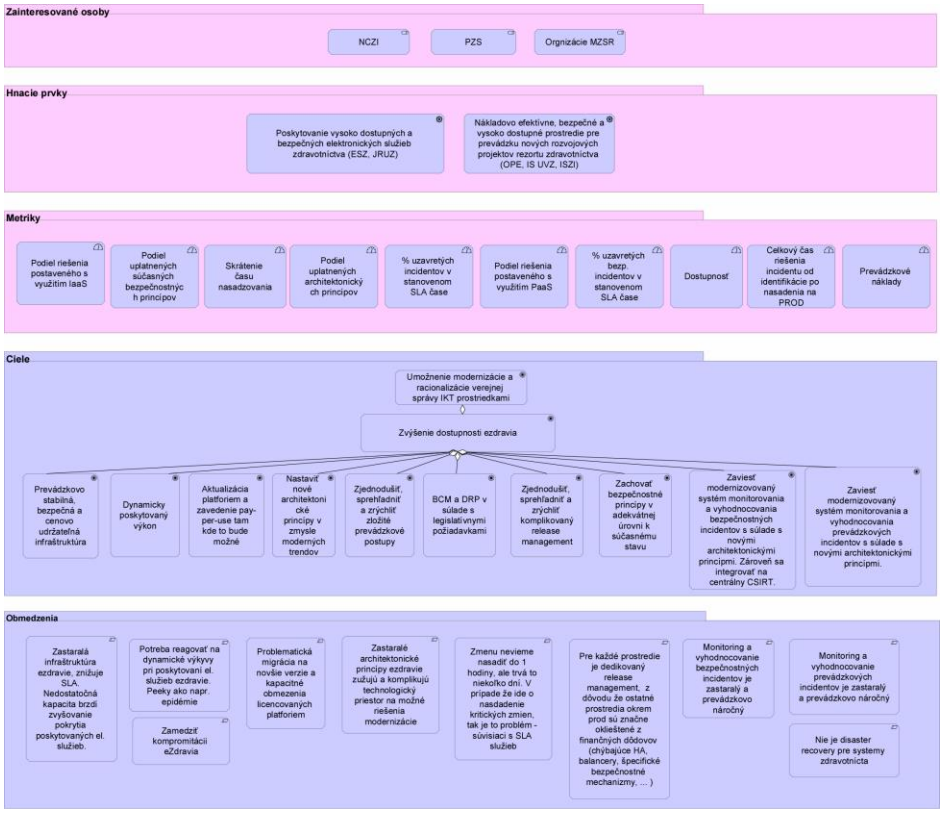
Z vyššie uvedených požiadaviek boli identifikované nasledujúce spoločné obmedzenia a príležitosti na zlepšenie

Obmedzenie	**Príležitosť na zlepšenie**
1.Zastaraná infraštruktúra - Ezdravie beží na zastaranej HW a SW infraštruktúre , ktorá bola nakupovaná v rozmedzí rokov 2009 až 2013. Riešenie síce beží vo vysokej dostupnosti na 2 vetvách, avšak výpadok jednotlivých prvkov sa stáva pomerne častou záležitosťou. Rovnako mnohé prvky sú už od výrobcov nepodporované. Preto prevádzka mitiguje na dennej báze riziká spojené s výpadkami. Pre nové projekty je potrebné pripraviť kapacitne a technologicky nové riešenie, ktoré umožní ich nasadenie do prevádzky.	Vybudovať bezpečnú a kapacitne dostatočnú infraštruktúru ezdravie
2.Obmedzený dynamicky poskytovaný výkon – Prevádzka elektronických služieb zdravotníctva poukázala na problém tzv. peakov, kde počas napr. zvýšeného chrípkového obdobia je dopyt po volaní služieb nárazový v podobe zvýšených návštev u lekára a následného zvýšeného počtu predpísaných a vybraných receptov.	Infraštruktúra poskytovaná formou služby na vyžiadanie (IaaS)
3.Zastaraný dizajn platforiem a problematická migrácia na novšie verzie – Vzhľadom na udržateľnosť existujúceho riešenia 5 rokov je potrebné po ukončení tohto obdobia vykonať redizajn riešenia na úrovní platforiem a použitých SW a vykonať upgrade na novšie verzie a tak uplatniť modernejšieho technológie v riešení, čo umožní optimalizáciu riešenia s dopadom aj na optimalizáciu prevádzky.	Platformy poskytované formou služby na vyžiadanie (PaaS)
4.Zastarané architektonické princípy – Riešenie vychádza zo schválenej architektúry na prelome rokov 2010 a 2011. Odvtedy sa posunuli trendy a technológie významne dopredu. Rovnako boli stanovené nové architektonické, bezpečnostné a iné princípy v zmysle NKIVS a nových zákonov o KB a GDPR, ktoré existujúce riešenie reflektuje len čiastočne.	Vybudovanie novej systémovej architektúry
5.Chýbajúci disaster recovery – Riešenie nemá záložné DC, čo pre takýto systém pre prácu s tak	Vybudovanie záložného riešenia, príprava DRP a BCM postupov a ich

citlivými dátami a potrebnými dátami pre rozhodovanie lekára je absolútna nutnosť. Lekári už dnes netlačia recepty a v prípade, že by došlo najhoršiemu scenáru výpadku primárneho DC je obnova časovo skôr ako do mesiaca nemožná v prípade, že by bola dostupná okamžitá vyhovujúca infraštruktúra v inom DC.	aplikácia. Zavedenie služieb zálohovania a obnovy zálohy. Je predmetom maximalistickej varianty, čo bude riešené v ďalšej etape rozvoja ezdravie.
6.Riziko kompromitácie ezdravia – v kontexte ostatných problémov sa zvyšuje riziko, že dôjde k bezpečnostnému incidentu, ktorý by kompromitoval samotné riešenie. Dopad z neho vyplývajúci by mohol spochybniť bezpečnosť riešenia ako takého.	Posúdenie systémovej architektúry Nový model hrozieb Návrh komplementárnych bezpečnostných princípov Návrh novej bezpečnosti SDL v.2 Aktualizovaný bezpečnostný projekt Nezávislý audit bezpečnosti
7.Zastaraný monitoring bezpečnostných incidentov – ako východisko je vnímanie problému č.4, kde aj bezpečnosť musí prejsť revíziou a novým vyhodnotením modelu hrozieb a aplikovaním nových opatrení tak aby sa reflektovali najnovšie modely hrozieb. Následne je potrebné aplikovať nové prevádzkové procesy do praxe a nastaviť nový monitoring. Existujúce riešenie neumožňuje integráciu s pripravovanými riešenia na úrovni eGOV.	Vybudovanie nového monitoringu bezpečnostných incidentov
8.Zastaraný monitoring prevádzkových incidentov – ako východisko je vnímanie problému č.4, kde aj prevádzka musí prejsť revíziou a novým vyhodnotením prevádzkového modelu a aplikovaním nových opatrení tak aby sa reflektovali najnovšie modely pre prevádzku nového riešenia. Následne je potrebné aplikovať nové prevádzkové procesy do praxe a nastaviť nový monitoring.	Vybudovanie nového monitoringu prevádzkových incidentov
9.Dlho trvajúci release manažment - zmenu nevieme nasadiť do 4 hodín, ale trvá to v niektorých prípadoch aj niekoľko dní. V prípade že ide o nasadenie kritických zmien, tak je to problém a má dopad SLA služieb. Preto dnes sme na úrovni dostupnosti služieb niekde okolo 95%.	Automatizovaný devops Posúdenie dopadov na existujúce riešenie a procesy
10.Chýbajúci automatizovaný devops a heterogenita prostredí - Pre každé prostredie je dedikovaný release management, z dôvodu že ostatné prostredia okrem produkčného sú značne okliešťené z finančných dôvodov. Takto nastavené	Automatizovaný devops Posúdenie dopadov na existujúce riešenie a procesy

riešenie si vyžaduje značné zdroje na prevádzku ale aj SLA. Heterogenita vedie k chybám, kde sa častou opravuje dodaný balíček a tak predlžuje čas.

Priestor pre sumárny obrázok: ArchiMate štandardný viewpoint – „Motivation viewpoint"



Merateľné ukazovatele KPI projektu pre identifikované požiadavky subjektov sú nastavené nasledovne:

Cieľ	**Požiadavka**	Súčasná hodnota	Cieľová hodnota	**Cieľový rok**
Prevádzkovo stabilná, bezpečná a cenovo udržateľná infraštruktúra BCM a DRP v súlade s legislatívnymi požiadavkami	Zlepšenie dostupnosti	95%	97,5%	2022
Prevádzkovo stabilná, bezpečná a cenovo udržateľná infraštruktúra BCM a DRP v súlade s legislatívnymi požiadavkami	Znížené prevádzkové náklady na každý IS s využitím výhod nových IaaS a PaaS služieb	100%	80%	2022
Dynamicky poskytovaný výkon	Podiel riešení s využitím IaaS služieb	0%	75%	2022
Aktualizácia platforiem a zavedenie pay-per-use tam kde to bude možné	Podiel riešení s využitím PaaS služieb	0%	75%	2022
Nastavenie nových architektonických princípov v zmysle moderných trendov	Podiel uplatnených nových architektonických princípov	0%	75%	2022
Zachovanie bezpečnostných požiadaviek v adekvátnej úrovni k súčasnému stavu	Podiel uplatnených súčasných bezpečnostných požiadaviek	100%	100% (20% pôvodné bezpečnostné princípy +80% nové komplementárne bezpečnostné princípy)	2022
Zavedenie modernizovaného systému monitorovania a vyhodnocovania bezpečnostných incidentov v súlade s novými architektonickými princípmi. Zároveň sa integrovať na centrálny CSIRT	% uzavretých bezpečnostných. incidentov v stanovenom SLA čase	75%	90%	2022

Zavedenie modernizovaného systému monitorovania a vyhodnocovania prevádzkových incidentov s súlade s novými architektonickými princípmi.	% uzavretých incidentov v stanovenom SLA čase	75%	90%	2022
Zjednodušenie, sprehľadnenie a zrýchlenie zložitých prevádzkových postupov	Skrátenie času nasadzovania incidentu typu A max. 24 hodín od identifikácie po nasadenie na PROD	100%	20%	2022
Zjednodušenie, sprehľadnenie a zrýchlenie komplikovaného release managementu	Celkový čas riešenia incidentu od identifikácie po nasadenia na PROD	5 dní	1 deň	2022

Špecifické ukazovatele výsledku programu zodpovedajúce špecifickému cieľu 7.8

P. č.	Ukazovateľ	Merná jednotka	Kategória regiónu	Východisková hodnota	Východiskový rok	Cieľová hodnota	Zdroj údajov	Interval vykazovania
1.	Celkové náklady na vlastníctvo ISVS	%	Menej rozvinuté regióny	100	2013	90	SORO	Ročne

Riziká

Spresnenie identifikovaných rizík:
R_16, R_20, R_21

- R_20 Nedostatočná spolupráca a súčinnosť organizácií v rámci rezortu zdravotníctva vo fáze analýzy a dizajnu projektu môže mať dopad na vývoj funkcionalít projektu.
- R_21 Nedostatočný záujem o využitie služieb zo strany projektov a organizácií rezortu zdravotníctva. Nedostatočné využitie ohrozuje naplnenie cieľov projektu a realizáciu úspor.
- R_16 Riziko nedosiahnutia plánovaných kvalitatívnych prínosov projektu.

Prílohy

Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.

Diagramy, modely, obrázky v plnom rozlíšení

Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

Popis aktuálneho stavu

Legislatíva

Tabuľka 4 Legislatíva – aktuálny stav

Súhrnný popis

Legislatívu v zdravotníctve definuje niekoľko legislatívnych noriem, ktoré definujú jednotlivé inštitúcie v rezorte a ich role v súvislosti s vytváraním, spravovaním a poskytovaním údajov. Zároveň legislatívne normy upravujú aj oblasť zdravotného informačného systému, štandardy zdravotníckej informatiky a hlásenia do národných registrov a štatistických výkazov.

Nariadenia Európskej únie:

- Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu
- Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)

Zákony:

- Zákon č. 153/2013 Z. z. o národnom zdravotníckom informačnom systéme
- Zákon č. 581/2004 Z. z. o zdravotných poisťovniach, dohľade nad zdravotnou starostlivosťou
- Zákon č. 355/2007 Z. z. o ochrane, podpore a rozvoji verejného zdravia
- Zákon č. 578/2004 Z. z. o poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve
- Zákon č. 362/2011 Z. z. o liekoch a zdravotníckych pomôckach
- Zákon č. 576/2004 Z. z. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti
- Zákon č. 538/2005 Z. z. o prírodných liečivých vodách, prírodných liečebných kúpeľoch, kúpeľných miestach a prírodných minerálnych vodách a o zmene a doplnení niektorých zákonov
- Zákon č. 577/2004 Z. z. o rozsahu zdravotnej starostlivosti uhrádzanej na základe verejného zdravotného poistenia a o úhradách za služby súvisiace s poskytovaním zdravotnej starostlivosti
- Zákon č. 579/2004 Z. z. o záchrannej zdravotnej službe
- Zákon č. 580/2004 Z. z. o zdravotnom poistení
- Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci

Okrem toho sú ďalšími relevantnými zákonmi zákonné normy a nariadenia EÚ týkajúce sa bezpečnosti:

- Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy
- Zákon č. 18/2018 Z. z. o o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
- Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

Ďalšie legislatívne normy dotýkajúce sa oblasti údajov v zdravotníctve zahŕňajú:

Vyhlášky a výnosy:

- Vyhláška č. 9/2014 Z. z. – Vyhláška MZ SR, ktorou sa ustanovujú podrobnosti o postupe, metódach, okruhu spravodajských jednotiek a lehotách hlásenia údajov do Národného registra zdravotníckych pracovníkov a jeho charakteristiky
- Vyhláška č. 74/2014 Z. z. – Vyhláška MZ SR, ktorou sa ustanovuje zoznam hlásení do národných zdravotných registrov, ich charakteristiky, podrobnosti o obsahu národných zdravotných registrov, postupe, metódach, okruhu spravodajských jednotiek a lehotách hlásení do národných zdravotných registrov
- Vyhláška 141/2016 Z. z. – Vyhláška MZ SR, ktorou sa mení a dopĺňa vyhláška Ministerstva zdravotníctva Slovenskej republiky č. 74/2014 Z. z.
- Vyhláška č. 10/2014 Z. z. – Vyhláška MZ SR, ktorou sa ustanovuje zoznam štatistických výkazov v zdravotníctve, podrobnosti o postupe, metódach, okruhu spravodajských jednotiek a lehotách hlásení v rámci štatistického zisťovania v zdravotníctve a ich charakteristiky
- Vyhláška č. 44/2014 Z. z. – Vyhláška MZ SR, ktorou sa ustanovujú podrobnosti o postupe, metódach, okruhu spravodajských jednotiek a lehotách hlásení pri zisťovaní udalostí charakterizujúcich zdravotný stav populácie a ich charakteristiky
- Vyhláška č. 107/2015 Z. z. – Vyhláška MZ SR, ktorou sa ustanovujú štandardy zdravotníckej informatiky a lehoty poskytovania údajov
- Výnos MF SR č. 55/2014 o štandardoch pre informačné systémy verejnej správy

Zmluvy:

- Kontrakt medzi NCZI a MZ SR o plnení úloh v oblasti informatizácie zdravotníctva, správy národného zdravotníckeho informačného systému, štandardizácie zdravotníckej informatiky, zdravotníckej štatistiky a poskytovania knižnično-informačných služieb v oblasti lekárskych vied a zdravotníctva.

Dokumenty:

- *Národná koncepcia informatizácie verejnej správy Slovenskej republiky – ďalej iba „NKIVS“*
- Strategické priority a dokumenty z pracovných skupín Národnej koncepcie informatizácie verejnej správy

Priestor pre sumárny obrázok / graf / diagram, nepovinná informácia.

Ďalšie informácie
(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)

Riziká **Spresnenie identifikovaných rizík:** *R_21*

- R_21 Nedostatočný záujem o využitie služieb zo strany projektov a organizácií rezortu zdravotníctva. Nedostatočné využitie ohrozuje naplnenie cieľov projektu a realizáciu úspor.

Prílohy	**Diagramy, modely, obrázky v plnom rozlíšení**
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	*Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*

Architektúra

Biznis architektúra

Tabuľka 5 Biznis architektúra - aktuálny stav

Súhrnný popis

Biznis architektúra zachytáva predstavu všetkých stakeholderov o tom, ako má NZIS fungovať. Snahou je poskytnúť také produkty a služby, ktoré pomôžu realizovať biznis procesy vykonávané aktérmi čo najpohodlnejším a najefektívnejším spôsobom. Funkcionalita z biznis pohľadu je to, čo vidí koncový používateľ systému, a preto musí byť dôkladne prediskutovaná a zladená, aby dokázala optimalizovať chod zdravotníctva, predísť neefektivitám, uspokojiť potreby odborného personálu a zabezpečiť kvalitnú zdravotnú starostlivosť pacientom. Návrh biznis architektúry vychádza zo súčasnej situácie, ktorú nadstavuje a vylepšuje podľa vízie optimálneho a pokrokového fungovania elektronického zdravotníctva.

Systém eZdravie bol nasadený do prevádzky od 1.1.2018. Aktuálne poskytuje nasledovné funkcie:

- Prístup do systému eZdravie – funkcia umožňuje prístup ZPr do systému eZdravie prostredníctvom ePZP, ktorý slúži zároveň aj ako elektronická pečiatka. Taktiež umožňuje prístup občana do systému eZdravie, a to prostredníctvom eID, ktorým môže cez portál NPZ vstúpiť do svojej EZK.
- eVyšetrenie – funkcia umožňuje tvorbu elektronického záznamu z vyšetrenia, ktorý následne ZPr podpíše prostredníctvom ePZP. Elektronický záznam sa ukladá do systému eZdravie. Pacient už nemusí nosiť papierovú zdravotnú dokumentáciu (napr. ak je poslaný lekárovi špecialistovi) a má prístup k svojej zdravotnej dokumentácii prostredníctvom EZK na portáli NPZ. Do systému eZdravie sú ukladané nasledovné záznamy:
    - záznam z odborného vyšetrenia
    - prepúšťacia správa
    - popis zo zobrazovacieho zariadenia (RTG, MR a iné)
    - výmenný lístok viazaný na odborné vyšetrenie Všeobecný lekár má prístup k celej zdravotnej dokumentácii pacienta, okrem záznamov vytvorených lekárom v špecializačnom odbore psychiatria alebo klinická psychológia – na základe rodného čísla (RČ).

  Lekár – špecialista má prístup len k informáciám o vyšetrení na základe výmenného lístka. K pacientskemu sumáru má lekár – špecialista prístup na základe rodného čísla po podpise informovaného súhlasu. Lekár - špecialista môže pristupovať k celej pacientovej zdravotnej dokumentácii, ale len na základe udelenia súhlasu na prístup samotným pacientom.

  Zdravotnícky pracovník záchrannej zdravotnej služby (iný ako lekár) má prístup k pacientskemu sumáru (tzv. život zachraňujúcim údajom) bez súhlasu pacienta a informovaného súhlasu.

- eRecept – funkcia prispieva k lepšiemu zdieľaniu zdravotných záznamov medzi oprávnenými lekármi, umožňuje oprávnenému lekárovi vidieť aktuálne lieky pacienta, históriu liečby, výrazne obmedzuje a časom úplne odstráni nutnosť tlačiť recepty či poukazy. Dovoľuje v rámci zdieľania informácií o predpisoch a histórie pacienta, overiť už pri predpise liekové interakcie. Systém môže na základe dát dostupných v reálnom čase upozorniť lekára na duplicity, ktoré môžu vzniknúť, ak lekári o predpisoch vzájomne nevedia. Zároveň eRecept zvyšuje bezpečnosť pacienta pri liečbe.

Lekár vykonáva predpis rovnako ako doteraz, avšak na pozadí v systéme sa realizuje kontrola, ktorá mu poskytuje informácie o potenciálnych liekových interakciách či duplicitách. Lekár si overuje na základe rodného čísla príslušnosť pacienta k ZP a jeho status dlžníka na zdravotnom poistení. Pri predpisovaní lieku dostáva lekár informáciu, či predpísané lieky, ktoré pacient používa nie sú vo vzájomnej interakcii, ktorá by mohla pacientovi ublížiť. Upozornenie sa objaví ešte pred potvrdením predpísania lieku a lekár môže podľa uváženia zohľadniť. Lekár vytvára elektronický preskripčný záznam, použitím ePZP sa nahrádza pečiatka a podpis lekára. Na jednom recepte môže byť iba jeden liek alebo jedna dietetická potravina. eRecept nie je potrebné tlačiť, v niektorých prípadoch však môže byť aj vytlačený. Lekár môže predpísať prostredníctvom eReceptu aj individuálne pripravované lieky. Lekár môže opraviť alebo zrušiť predpis. Oprava sa môže vykonať iba tak, že lekár pôvodný predpis stornuje a vystaví nový. Oprava aj zrušenie elektronického preskripčného záznamu sú možné iba dovtedy, pokiaľ lekáreň na základe tohto elektronického preskripčného záznamu nezrealizovala elektronický výdaj vo svojom softvéri.

Pacient nemusí mať v lekárni k dispozícii papierový recept/poukaz. V lekárni alebo výdajni predloží svoj preukaz poistenca, z ktorého si lekárnik zistí RČ, ktoré zadá do systému. Alebo vloží svoj eID do čítačky, čím sa automaticky overí identita pacienta. Lekárnik môže overiť identitu pacienta aj prostredníctvom načítania čiarového kódu z papierového predpisu. Po identifikácii pacienta zobrazí systém lekárnikovi alebo výdajcovi zdravotníckych pomôcok všetky jeho predpísané nevydané lieky/zdravotnícke pomôcky/dietetické potraviny. Lekárnik vyberie elektronický preskripčný záznam s tým liekom/pomôckou/dietetickou potravinou, ktorý si pacient aktuálne prišiel vybrať. Následne výdaj bezodkladne po jeho zrealizovaní potvrdí aj v softvéri, čím sa na pozadí odošle informácia, online, do systému eZdravie.

Lekárnik môže upraviť údaje z elektronického preskripčného záznamu, v súlade s platnou legislatívou tak, že uvedie správne údaje v elektronickom dispenzačnom zázname. Opravu alebo zmenu údajov o výdaji lekárnik realizuje čo najskôr tak, že pôvodný elektronický dispenzačný záznam v softvéri vystornuje a vytvorí nový elektronický dispenzačný záznam so správnymi údajmi. Záznam sa dá zrušiť aj kompletne - vystornovaním.

Po novom je taktiež možne využívať tzv. opakovaný recept, ktorý prispieva k zníženiu počtu pacientov v čakárňach ambulancií, pomáha ušetriť čas lekárom, sestrám aj pacientom a prispieva k odstráneniu papierových predpisov. Lekár po posúdení zdravotného stavu pacienta na predpis opakovaného eReceptu, predpíše dávku liekov na jeden výber, určí platnosť receptu maximálne na 365 dní od dátumu predpisu, určí koľko dní musí uplynúť medzi dvoma výbermi na základe opakovaného eReceptu (perióda opakovania, najviac 3 mesiace, napríklad 30 dní) a určí počet možných výberov (2 a viac). Predpis je výlučne elektronický a lekár musí mať softvér s overením zhody pre funkcionalitu na predpisovanie opakovaných eReceptov. Zoznam liekov, ktoré nie je možné na opakovaný eRecept predpísať, stanovuje vyhláška. Po uplynutí lekárom stanoveného obdobia sa recept objaví v zozname nevydaných liekov v lekárni a bude k dispozícii dovtedy, kým si pacient danú dávku nevyzdvihne, najneskôr však do konca platnosti opakovaného eReceptu. Pacient nemusí prísť presne v deň uplynutia periódy, ale vzhľadom na riadne dodržiavanie lekárom stanoveného liečebného režimu, má pacient vyberať a užívať lieky pravidelne. Ak pacient zabudol, kedy si má lieky na opakovaný eRecept vybrať, môže si v lekárni overiť či sú už preňho k dispozícii nevydané lieky na

platné predpisy. V bežnom živote pacient zistí, že mu lieky došli a ak má opakovaný eRecept, stačí, že navštívi lekáreň a lieky si vyberie. Ušetrí tak čas potrebný na nový predpis. Ak by sa pacientovi zmenil zdravotný stav, riadne navštívi svojho lekára a ten rozhodne o ďalšom postupe presne tak isto, ako doteraz. Z pohľadu lekárne nedochádza pri výdaji liekov k žiadnym zmenám. Po identifikácii pacienta lekárnik načíta zoznam platných a nevydaných receptov a tie, ak ich má na sklade, riadne vydá a pomocou svojho softvéru zaznačí príslušné výdaje liekov. Vydávané sú množstvá do maximálnej, lekárom predpísanej výšky, pre jeden výber. Pri opakovanom eRecepte sa výdajom automaticky aktivuje možnosť ďalšieho výberu, po uplynutí príslušnej periódy medzi výbermi, tak ako to určil predpisujúci lekár. Pred uplynutím tejto periódy výber nie je možný. Ak opakovaný eRecept obsahuje „nevyčerpané“ dávky, príslušná dávka sa buď zobrazí v zozname nevydaných liekov alebo bude pri danom predpise uvedený dátum, kedy najskôr je možné príslušný liek vybrať. Po vypršaní platnosti opakovaného eReceptu, nie je ďalší výber možný a pacient musí navštíviť lekára, ktorý v prípade potreby predpis vystaví znova.

Ak lekáreň nemá predpísaný liek pacienta na sklade, môže ho objednať a následne dodať, pričom eRecept počas tohto procesu zablokuje. Takýto postup má zabrániť duplicitne vydávaným liekom vo viacerých lekárňach. Lekáreň v softvéri potvrdí blokovanie predpisu lieku, čím automaticky zablokuje jeho výdaj v inej lekárni. Dobu blokovania určí zdravotná poisťovňa na základe platnosti predpisu a nastavenia maximálnej doby pre výdaj. Doba je nastavená tak, aby neprevyšovala čas platnosti predpisu. Ak lekáreň nevie požadovaný liek v tomto čase vydať, predpis odblokuje. Blokovaný eRecept sa automaticky odblokuje pri reálnom výdaji lieku.

- eObjednanie - funkcia, ktorá umožňuje pacientom objednať sa k lekárovi cez internet počas doplnkových ordinačných hodín (DOH) na konkrétny dátum a čas, prípadne vytvoriť požiadavku o pridelenie termínu počas ordinačných hodín, tzv. objednávku do poradovníka ambulancie.
- eMedikácia - funkcia, ktorá umožňuje viesť medikačnú históriu pacienta vrátane podanej medikácie v ústavnej zdravotnej starostlivosti
- eLab - funkcia, ktorá umožňuje zápis laboratórneho vyšetrenia laboratóriom do EZK a jeho sprístupnenie pre PZS a ZPr. Bol adoptovaný medzinárodný číselník laboratórnych položiek LOINC do štruktúr výsledkov, ktorý umožni lepšiu komunikáciu medzi ZPr a laboratóriami a následne aj transparentnejšie vykazovanie.
- elektronická zdravotná knižka (EZK) – funkcia evidencie zdravotných záznamov v elektronickej zdravotnej knižke (EZK) predstavujú nevyhnutnú výbavu pre ošetrujúcich zdravotníckych pracovníkov na stanovenie úspešnej diagnózy a následnej terapie. ZPr nájde v EZK všetky potrebné informácie pre anamnézu, diagnostiku a terapiu. Do EZK pristupuje zo svojho informačného systému. Pacient má vďaka EZK informácie o svojom zdravotnom stave online a kedykoľvek k dispozícii. Podmnožinou EZK je pacientsky sumár, ktorý umožňuje rýchly prístup ku najdôležitejším údajom pacienta pre poskytnutie zdravotnej starostlivosti.
- Národný portál zdravia (NPZ) je vstupnou bránou do EZK. Zároveň je to webová stránka, obsahujúca aplikácie, ako aj dôveryhodné aktuálne a autorizované informácie súvisiace so zdravotnou starostlivosťou a službami spojenými s jej poskytovaním. Nachádzajú sa tu tiež informácie o ohrozeniach zdravia, chorobách, liekoch, diagnostike a liečení chorôb, poskytovateľoch zdravotnej starostlivosti, a aj o legislatíve v zdravotníctve. Na webovej

stránke NPZ je odkaz na "Moja zdravotná knižka". Po kliknutí na odkaz sa otvorí informácia o nutnosti inštalácie aplikácie eID. Ak je aplikácia eID nainštalovaná, pokračujete v prihlásení do EZK prostredníctvom zadania BOK (bezpečnostný ochranný kód). Elektronická zdravotná knižka (EZK) obsahuje záznamy vytvorené ZPr, pričom každý záznam zároveň obsahuje identifikačné údaje ZPr, ktorý ho vytvoril a jeho elektronický podpis. Nájdete tu tiež údaje z účtu poistenca a vlastné záznamy pacienta. Každý prístup, pokus o prístup či poskytnutie údajov je v EZK zaznamenané. Občan tak má vedomosť o prístupoch k jednotlivým elektronickým zdravotným záznamom.

EZK je rozdelená do nasledovných priečinkov:

a) Osoba - obsahuje identifikačné údaje osoby, ktorej EZK patrí, t. j. základné informácie o pacientovi.

b) Pacientsky Sumár - obsahuje základné život zachraňujúce údaje o pacientovi:

- údaje o implantovanej zdravotníckej pomôcke, vrátane údajov o zubno-lekárskej zdravotníckej pomôcke (napr. zubný implantát)
- údaje o alergiách
- kontaktné údaje pacientovho všeobecného lekára
- kontaktné údaje iného ošetrujúceho lekára, ktorého si vyberie pacient
- kód a názov choroby a jej bližšiu špecifikáciu, ak pacient trpí niektorou z chorôb, uvedených v zozname chorôb stanovených vyhláškou Ministerstva zdravotníctva SR, ktoré sa zapisujú do pacientskeho sumára a ktorá je na základe posúdenia ošetrujúceho lekára dôležitá z hľadiska záchrany života a zdravia osoby
- údaje o podaných a vydaných liekoch
- údaje o kontaktnej osobe určenej pacientom
- predpokladaný dátum pôrodu

c) Očkovania - obsahuje údaje o vykonaných očkovaniach pacienta.

d) Liečba - obsahuje údaje o spôsobe liečby pacienta.

e) Laboratórne vyšetrenia – v priečinku sa nachádzajú pacientove výsledky laboratórnych vyšetrení.

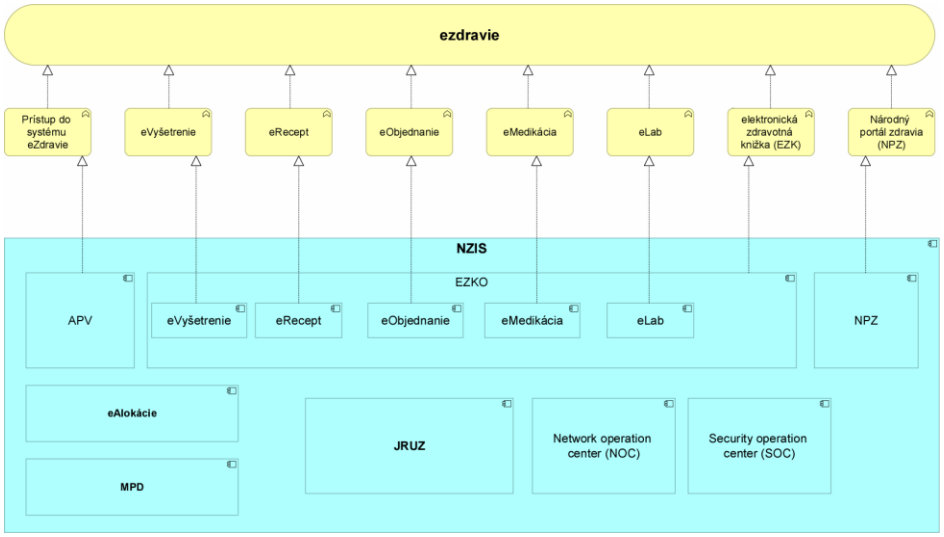
f) Vyšetrenia - Priečinok zhromažďuje popisy prípadných zdravotných ťažkostí pacienta, ako aj popisy jeho vyšetrení, stanovenie diagnóz a navrhované liečby.

g) Recepty - V priečinku sa nachádza zoznam liekov, ktoré lekári pacientovi predpísali.

h) Voľnopredajné lieky - Priečinok obsahuje pacientove záznamy o liekoch, ktoré užíval.

i) Doplňujúce informácie - V tomto priečinku sa nachádzajú doplňujúce informácie o pacientovi.

Priestor pre sumárny obrázok: ArchiMate štandardný viewpoint – „Product viewpoint", „Business Process Viewpoint"



Ďalšie informácie
(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)

Riziká

Spresnenie identifikovaných rizík: *R_1, R_17*

- R_1 Neoptimálne procesy prevádzky
- R_17 Zabezpečenie dostupnosti informačných systémov (najmä v prípade rozsiahlych havárií - disaster) nezodpovedá legislatívnym požiadavkám

Prílohy

Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.

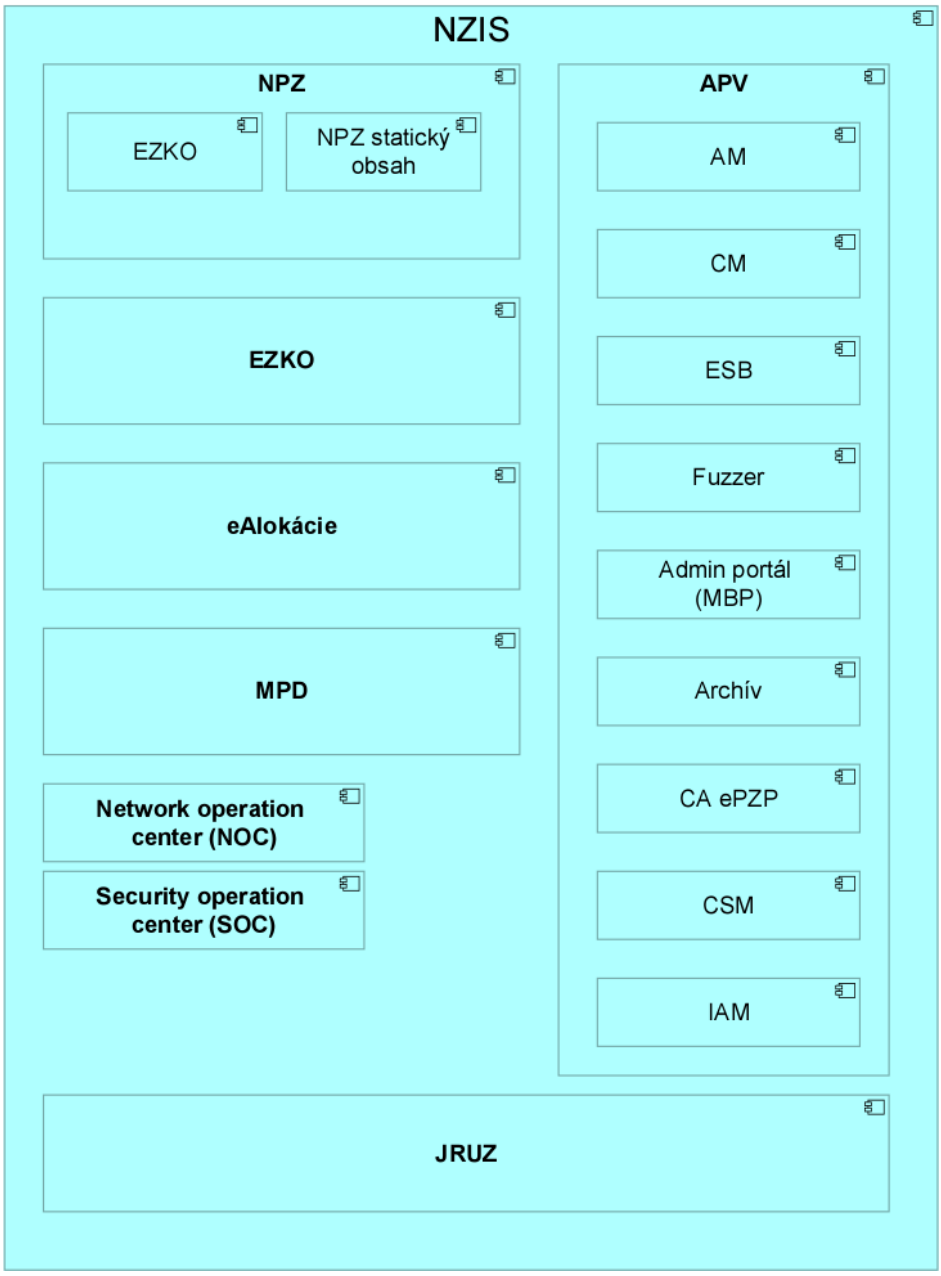
Diagramy, modely, obrázky v plnom rozlíšení

Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

Architektúra informačných systémov

Tabuľka 6 Architektúra informačných systémov - aktuálny stav

Súhrnný popis

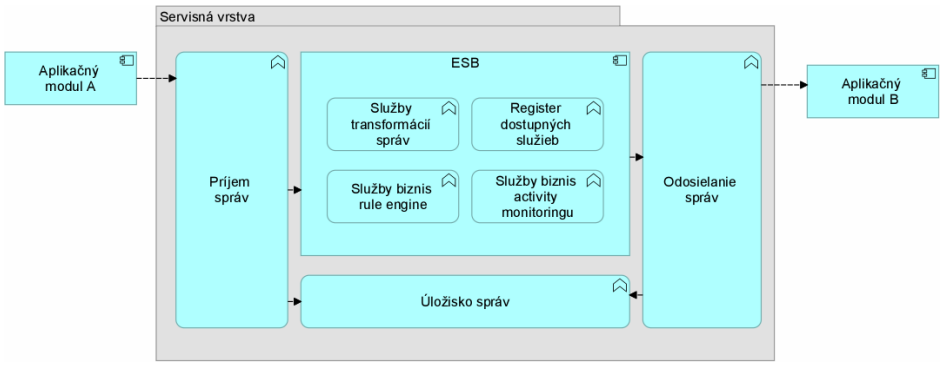


Obrázok - Aplikačná architektúra NZIS

Servisná vrstva

Servisná vrstva (ďalej len „ESB vrstva“) sprostredkúva komunikáciu jednotlivých modulov systému a zabezpečuje vrstvu abstrakcie medzi nimi. ESB vrstva zabezpečuje zaručené smerovanie a doručenie správy na cieľové služby a prispôsobenie formátu správy, ak je to

potrebné. Správy prijaté z externého systému sú ukladané do databázy, v ktorej zostávajú do úspešného doručenia na cieľovú službu. ESB vrstva taktiež zabezpečuje synchrónnu a asynchrónnu komunikáciu s externými systémami (vypublikovaním jej služieb vzniká Servisné rozhranie pre externé systémy).



Obrázok - Servisná vrstva

ESB vrstva taktiež obsahuje služby, ktoré môžu aplikačné moduly využívať:

1) Register dostupných služieb

2) Služby biznis activity monitoringu

3) Služby biznis rule engine

4) Služby transformácií správ

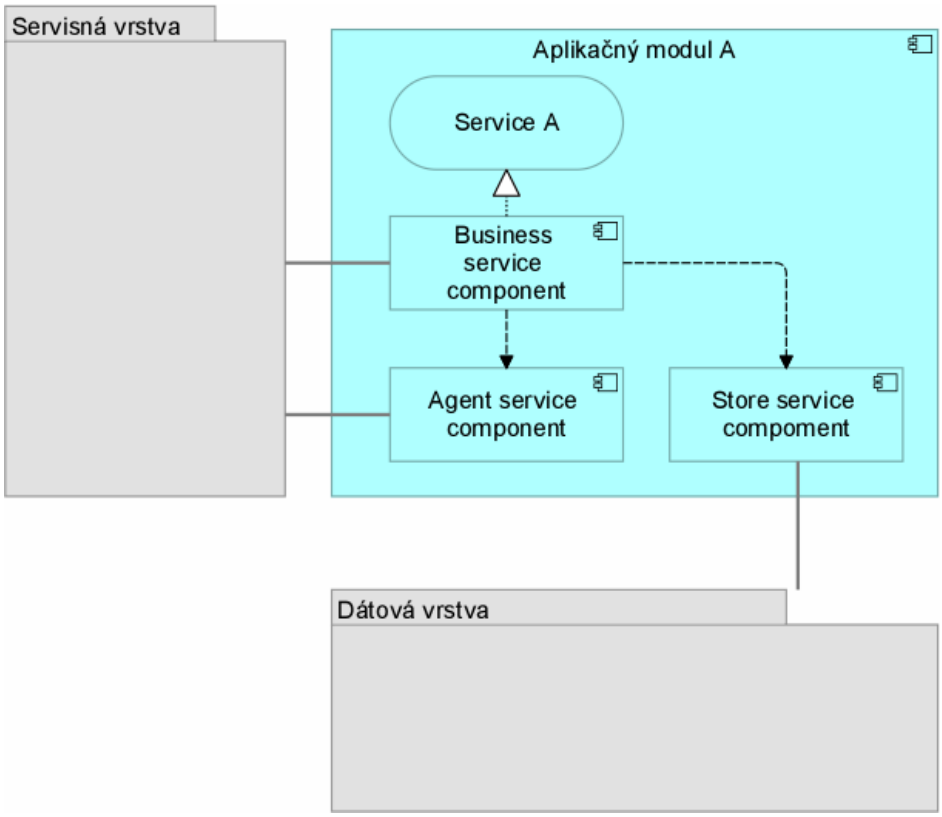
Vrstva biznis procesov

Vrstva obsahuje prostriedky pre správu dlho bežiacich biznis procesov. Vrstva zabezpečuje možnosť implementácie dlho bežiacich procesov spájajúcich (využívajúcich) služby viacerých aplikačných modulov a interagujúcich s externým prostredím. Typickým príkladom takejto služby je napríklad schvaľovanie lieku na špeciálnu objednávku, kde lekár žiada o liek, zdravotná poisťovňa liek schvaľuje, lekáreň liek objednáva, následne je lekár/pacient notifikovaný o dostupnosti lieku.

Pre potreby ESZ neboli takéto procesy identifikované, všetky služby ESZ majú atomický charakter. Vrstva je v architektúre uvádzaná pre využitie v ďalších fázach.

Vrstva aplikačných modulov

Vrstva aplikačných modulov pokrytie aplikačnej (back end) logiky navrhovanej v zmysle servisne orientovanej architektúry. Základná architektúra servisnej aplikácie je znázornená na nasledovnom obrázku:



Obrázok - Vrstva aplikačných modulov

Aplikačný modul pozostáva z nasledovných charakteristických vrstiev:

1. Businesss Service vrstva - zapuzdruje časť procesu, ktorý číta, vytvára a aktualizuje entity vo viacerých nezávislých funkčných doménach (využíva store service vrstvu). Nemá vlastné dáta.
2. Store Service vrstva - zabezpečuje životný cyklus entít a ich vzťahov v rámci danej funkčnej domény. Zabezpečuje prácu s perzistentnou podobou daných biznis entít.
3. Agent Service vrstva - zabezpečuje rozhranie na dáta mimo daného modulu. Z iného modulu získava dáta a zabezpečuje ich transformáciu. Do vnútra modulu poskytuje dáta v podobe, v akej sú pre modul prirodzené. Zabezpečuje vrstvu abstrakcie. V prípade, ak

sa rozhrania iných modulov v budúcnosti zmenia, zmena je lokalizovaná v tomto komponente a nenastáva vo vrstve business service.

Komunikácia medzi Business Service Component, Store a Agent Service Component v rámci aplikačného modulu prebieha priamo, bez sprostredkovania ESB vrstvy.

Priestor pre sumárny obrázok: ArchiMate štandardný viewpoint – „Application Usage Viewpoint", „Application Co-operation Viewpoint"

Ďalšie informácie
(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)

Riziká

Spresnenie identifikovaných rizík: *Odkazy na relevantné identifikátory rizík v prílohe Riziká.*

Stručná charakteristika identifikovaných rizík (Max. 400 znakov)

Prílohy

Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.

Diagramy, modely, obrázky v plnom rozlíšení

Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

Technologická architektúra

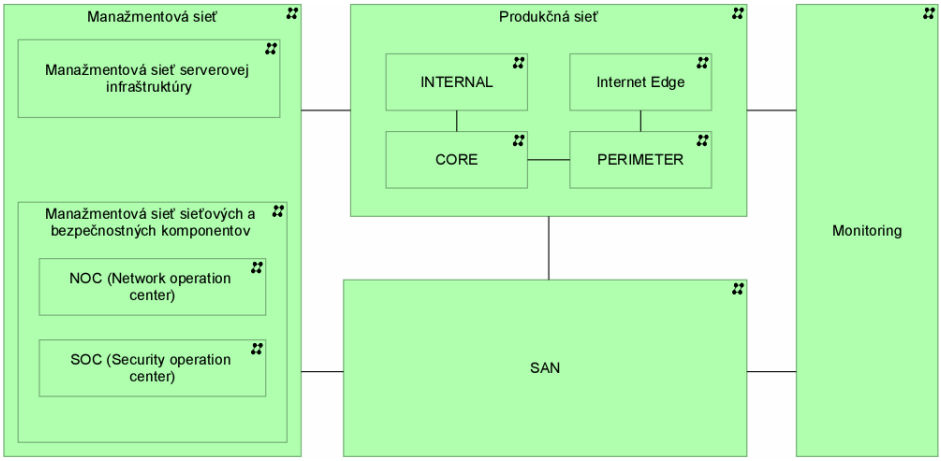
Tabuľka 7 Technologická architektúra - aktuálny stav

Súhrnný popis

Hlavné subsystémy a bloky riešenia sieťovej infraštruktúry

Sieťová infraštruktúra je rozdelená do nasledujúcich subsystémov a blokov. Každý z nich má špecifické vlastnosti a je dedikovaný na plnenie konkrétných úloh.

1. Produkčná sieťová infraštruktúra dátového centra
    1. Modul WAN a internet konektivity s podporou pripojenia na externé prostredie (Internet edge)
    2. Core vrstva sieťového prostredia
    3. Internal
        1. Agregačná vrstva sieťového prostredia
        2. Prístupová vrstva sieťového prostredia
        3. Servisná vrstva
    4. Perimeter
        1. Agregačná vrstva sieťového prostredia
        2. Prístupová vrstva sieťového prostredia
        3. Servisná vrstva
2. SAN infraštruktúra
3. Manažmentová sieť DC prostredia
4. Monitoring a správa sieťovej infraštruktúry



Obrázok - Logický pohľad na celkové riešenie sieťovej infraštruktúry

Produkčná sieťová infraštruktúra DC prostredia:

- Predstavuje infraštruktúru zabezpečujúcu komunikáciu jednotlivých produkčných komponentov IS ESZ.

Manažmentová sieť DC prostredia:

- Manažmentová sieť je dedikované sieťové prostredie zabezpečujúce komunikáciu prvkov realizujúcich správu zariadení umiestnených vo všetkých ostatných časti prostredia IS ESZ. Správa zariadení je realizovaná výlučne z tejto siete.

SAN infraštruktúra:

- SAN infraštruktúra je dedikované sieťové prostredie pre pripojenie a zabezpečenie komunikácie dátových úložísk a zálohovacích komponentov so serverovými komponentmi umiestnenými v produkčnej časti prostredia IS ESZ.

Monitoring a správa sieťovej infraštruktúry:

- Oblasť obsahuje komponenty zabezpečujúce prevádzkové aspekty sieťovej infraštruktúry IS ESZ akými sú správa, monitoring, zálohovanie konfigurácií, change management, aktualizácie a iné.

Produkčná sieťová infraštruktúra DC prostredia

Pre potreby vytvorenia blokov a zón na úrovni produkčnej sieťovej infraštruktúry DC je fyzický pohľad rozdelený do dvoch hlavných logických blokov. Tieto bloky sú pre potreby riešenia nazvané Perimeter DC a Internal DC.

Perimeter DC obsahuje zóny vystavené komunikácii z modulu Internet edge. Internal DC obsahuje zóny komunikácie jedine so zónami umiestnenými takisto v internal DC, alebo v perimeter DC.

V oboch blokoch je zachované hierarchické rozdelenie siete do vrstiev (agregačná, prístupová, servisná). Jediným spoločným prvkom je Core vrstva. Tá slúži na prepájanie Perimeter a Internal DC a ostatných zón produkčnej časti DC prostredia.

Okrem tohoto základného delenia na Internal DC a Perimeter DC je ešte realizované logické delenie vo vnútri týchto dvoch hlavných častí na jednotlivé zóny, ktoré je realizované logickou separáciou a to použitím technológie VRF a využitím kontextov na príslušných zariadeniach.

Priradenie samotných serverov resp. iných zariadení využívajúcich sieťovú infraštruktúru produkčnej časti DC do zón je na základe sieťového rozhrania na sieťovom prvky priradenom do danej zóny.

SAN infraštruktúra

V riešení je SAN infraštruktúra je tvorena nasledujúcimi blokmi:

- Edge vrstva pre servery z produkčnej časti siete DC

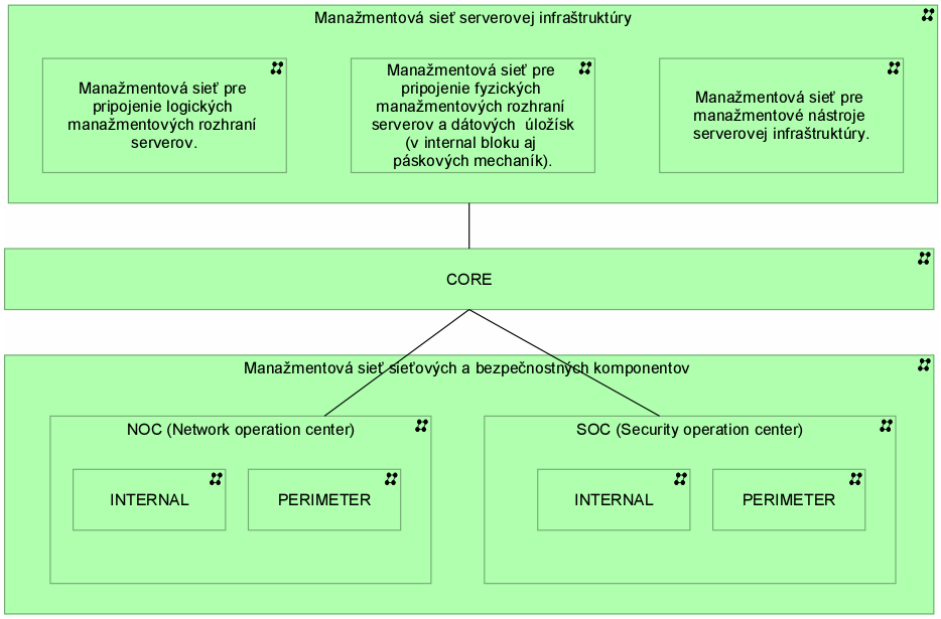
- Edge vrstva pre servery z manažmentovej siete bezpečnostných a sieťových komponentov (SOC, NOC)
- Core vrstva SAN
- Dátové úložiská

Manažmentová sieť DC prostredia

Pre správu zariadení je vytvorená dedikovaná manažmentová sieť. Manažmentová sieť je oddelenou sieťou od produkčnej siete a slúži na administráciu a manažovanie zariadení v sieti DC.

Manažmentová sieť je členená na dve hlavné časti:

- Manažmentová sieť bezpečnostných a sieťových komponentov
- Manažmentová sieť serverovej infraštruktúry



Obrázok - Logické členenie manažmentovej siete

Manažmentová sieť bezpečnostných a sieťových komponentov sa ďalej delí na dve časti:

- SOC - Security Operations Center
- NOC - Network Operations Center

Manažmentová sieť serverovej infraštruktúry sa ďalej delí na:

- Manažmentová sieť pre pripojenie logických manažmentových rozhraní serverov.
- Manažmentová sieť pre pripojenie fyzických manažmentových rozhraní serverov a dátových úložísk (v internal bloku aj páskových mechaník).
- Manažmentová sieť pre manažmentové nástroje serverovej infraštruktúry.

NOC a SOC sú realizované ako dedikované fyzicky oddelené prostredia. NOC taktiež poskytuje pripojenie pre fyzické manažmentové rozhrania serverov. Manažmentová sieť pre manažmentové nástroje serverovej infraštruktúry využíva zariadenia produkčnej časti siete, pričom oddelenie od produkčnej časti siete je na logickej úrovni.

Správa zariadení vrátane serverov a dátových úložísk je realizovaná výhradne z týchto sietí. Manažment zariadení modulu Internet edge je realizovaný Inband.

Monitoring a správa sieťovej infraštruktúry

Pre monitorovanie a správu sieťovej infraštruktúry sú využívané nasledujúce tri spôsoby:

- SW manažmentové nástroje vendora
- Priamy prístup na CLI zariadení s využitím SSH klient aplikácie

Priestor pre sumárny obrázok: ArchiMate štandardný viewpoint – „Infrastructure Usage Viewpoint", „Infrastructure Viewpoint"

Ďalšie informácie
(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)

Riziká **Spresnenie identifikovaných rizík:** *R_19*

R_19 Riziko zastaranej infraštruktúry a platforiem. Z pohľadu infraštruktúry NZIS, JRÚZ a ISZI má pomerne zastaralú infraštruktúru v niektorých prípadoch viac ako 10 ročnú bez možnosti zakúpenia supportu, čo predstavuje významné riziko z pohľadu výpadku IS. Rovnaká situácia je aj v podobe platforiem, kde riešenie beží na verziách vydaných cca 5 rokov starých.

Prílohy	**Diagramy, modely, obrázky v plnom rozlíšení**
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	*Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*

Bezpečnostná architektúra

Tabuľka 8 Bezpečnostná architektúra - aktuálny stav

Súhrnný popis

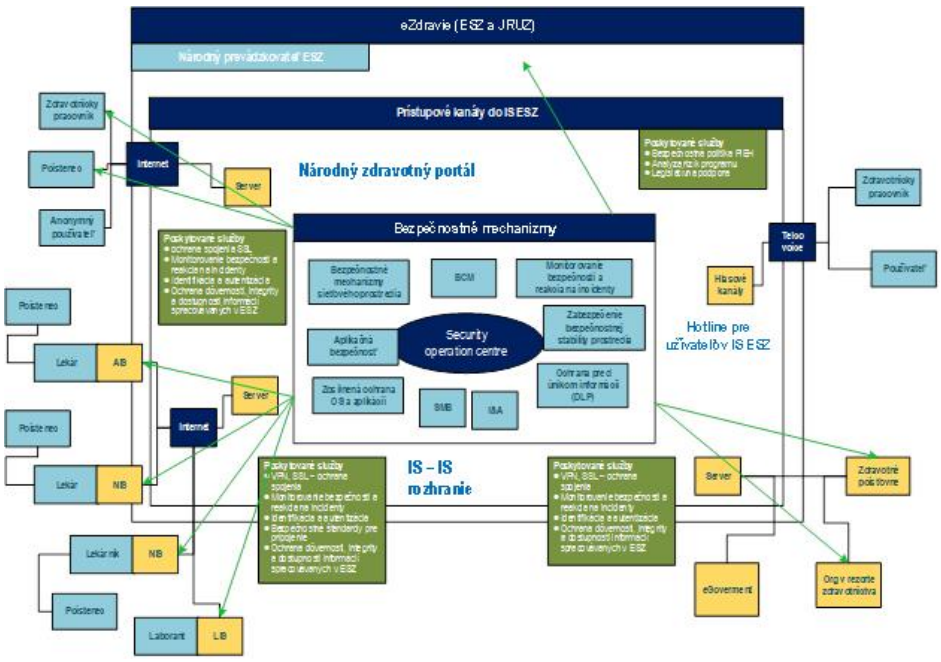
ESZ a taktiež NZIS sú informačným systémom verejnej správy, ktorého hlavným informačným aktívom sú informácie z pohľadu občanov najcitlivejšie t. j. údaje o zdravotnom stave, ktoré aj v zmysle zákona o ochrane osobných údajov spadajú pod osobitnú kategóriu osobných údajov.

V rámci ochrany zdravotných záznamov má veľký význam nielen dôvernosť, ale aj ich integrita a dostupnosť. Preto bezpečnosť v rámci ESZ zohľadňuje všetky tri aspekty – dôvernosť, dostupnosť a integritu s vysokou silou použitých bezpečnostných mechanizmov v rámci použitých komponentov. Úroveň požadovanej bezpečnosti vysoko prekračuje požiadavky na iné systémy v rámci eGovernmentu a má samozrejme dopad na rozsah a kvalitu použitých bezpečnostných komponentov, čo má samozrejme dopad aj na ich cenu.

Projekt ESZ realizuje unikátne bezpečnostné mechanizmy, ktoré sú schopné eliminovať riziko narušenia dôvernosti a úniku informácií zo strany administrátora. Tento cieľ bol dosiahnutý vďaka veľmi hlbokej implementácii bezpečnostných mechanizmov priamo do vyvíjaného softvéru a IS architektúry.

Bezpečnostná architektúra je realizovaná ako vzájomne úzko prepojený komplexný systém ochrany implementovaný technickými prostriedkami t. j. dedikovanými bezpečnostnými prostriedkami ako aj prostriedkami tvoriacimi súčasť aplikačných komponentov a infraštruktúry a netechnickými prostriedkami pre manažment informačnej bezpečnosti.

To umožnilo navrhnúť systém realizujúci ochranu do hĺbky, implementáciu a vynucovanie dodržiavania bezpečnostnej úrovne počas celého životného cyklu počínajúc už od úvodných fáz vývoja APV komponentov s osobitným dôrazom na ochranu osobných údajov. Architektúra technických prvkov je navrhnutá tak, aby v kooperácií s ostatnými oblasťami riešenia, ako napr. sieťová a aplikačná architektúra, umožnila stálu dostupnosť a škálovateľnosť.



Obrázok - Znázornenie bezpečnostnej architektúry a služieb poskytovaných do okolia

Jednotlivé bloky bezpečnostnej architektúry sú predstavované:

- **Aplikačnou bezpečnosťou**: Predstavuje mechanizmy, ktoré sú realizované application-aware prvkami, medzi ktoré patria COTS komponenty implementujúce aplikačnú logiku (web server, databázy, orchestračný mechanizmus atď.) a novo-vyvinuté aplikačné komponenty. Popisované mechanizmy sú vynucované, podporované a monitorované bezpečnostnými prvkami ostatných skupín. Cieľom je implementácia bezpečnostných čŕt do riešenia od začiatku vývoja a snaha využiť bezpečnostné mechanizmy dodávaného SW tretích strán. Kľúčovým aspektom je integrácia prvkov prinášaných NZIS s K + D konceptom implementovaným v ESZ tak, aby naďalej bola zabezpečená maximálna ochrana osobných údajov osobitnej kategórie predstavujúcich elektronické zdravotné záznamy.
- **SMIB**: Systém manažmentu (riadenia) informačnej bezpečnosti je podľa STN ISO/IEC 27001 časťou celkového systému riadenia, založený na prístupe k riziku organizácie, ktorého úlohou je zaviesť, implementovať, prevádzkovať, monitorovať, revidovať, udržiavať a zlepšovať informačnú bezpečnosť. Jedným z najvýznamnejších aktív v rámci eZdravie sú osobné údaje prijímateľov zdravotnej starostlivosti. Vzhľadom na to sa informačná bezpečnosť stáva nevyhnutnosťou.
- **Monitorovanie bezpečnosti a reakcia na incidenty:** Monitorovanie bezpečnosti je realizované dedikovaným Bezpečnostným dohľadovým centrom (SOC) zriadeným u Národného operátora eZdravie - NCZI. Ako hlavný technologický komponent pre monitorovanie je použitý SIEM produkt, umožňujúci centrálne monitorovanie a vyhodnocovanie bezpečnosti.
- **Bezpečnostné mechanizmy sieťového prostredia** sú v prostredí IS ESZ realizované segmentáciou prostredia do bezpečnostných zón na úrovni siete s definovanými prestupnými bodmi medzi zónami (tzv. choke points), ktoré riadia medzi-zónovú komunikáciu pomocou vynucovania definovanej bezpečnostnej politiky, vrátane aktivácie bezpečnostných mechanizmov na non-security zariadeniach a zabezpečenia dodatočnej ochrany komunikácie, ak je to potrebné. Úlohou bezpečnostných mechanizmov sieťového prostredia je taktiež zabezpečiť vytvorenie bezpečného komunikačného kanála pre komunikáciu s externými subjektmi - VPN formou vytvorenia centrálnych komponentov na strane IS ESZ.
- **Zabezpečenie bezpečnostnej stability** prostredia predstavuje mechanizmy zabezpečujúce monitorovanie a vynútenie integrity, verifikáciu stavu bezpečnosti vzhľadom na definovaný baseline a aktuálne hrozby. Všetky mechanizmy sú aplikované nielen počas prevádzky ESZ, ale aj počas fáz vývoja riešenia. Výstupy z fáz SLDC (napr. výstup z testovania) predstavujú podklad (baseline) pre kontrolu.
- **Ochrana pred únikom informácií** je riešená aj bezpečnostnými mechanizmami popísanými v ostatných blokoch bezpečnostnej architektúry, ale vzhľadom na fakt, že jednou z najvážnejších hrozieb je únik MC (mimoriadne citlivých - čo sú osobné údaje osobitnej kategórie predstavujúcich elektronické zdravotné záznamy) informácií, ako súčasť bezpečnostnej architektúry je potrebné v rámci ochrany do hĺbky vytvoriť

samostatný nezávislý prvok, ktorý zabezpečuje ochranu pred únikom informácii a ponúkne špecializovaný pohľad na úroveň zabezpečenia.

- **Zosilnenie ochrany operačných systémov a aplikácií predstavuje dôslednú realizáciu konceptu.** Ochrany do hĺbky: Využíva jednak natívne mechanizmy operačných systémov a aplikácií ako aj aditívne prvky predstavované dedikovanými bezpečnostnými softvérmi, ktoré pridávajú špecializované funkcionality, ako je napríklad behaviorálna detekcia škodlivého kódu.

Ochrana osobných údajov osobitnej kategórie predstavujúcich elektronické zdravotné záznamy sa riadi bezpečnostným projektom, ktorý bol vypracovaný na základe ustanovení zákona č. 122/2013 Z. z. o ochrane osobných údajov.

Priestor pre sumárny obrázok / graf / diagram.

Ďalšie informácie
(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)

Riziká

- R_18 Únik osobných a citlivých zdravotných údajov

Spresnenie identifikovaných rizík: *R_18*

Prílohy

Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.

Diagramy, modely, obrázky v plnom rozlíšení

Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

Prevádzka

Tabuľka 9 Prevádzka - aktuálny stav

Súhrnný popis

Monitoring ESZ – existujúci monitorovací nástroj je možné použiť len pre čiastkový monitoring infraštruktúry (sieťový, systémový a aplikačný). V rámci projektu NZIS môžu byť dáta existujúceho monitoringu použité ako zdroj pre centrálny monitoring biznis služieb. Vzhľadom na skutočnosť, že súčasný monitorovací nástroj nemožno použiť pre centrálny monitoring biznis služieb, ani ho nie je možné integrovať v rámci procesov riadenia prevádzky (Event Management), je možné hodnotiť aktuálny stav za nedostatočný.

Zálohovanie ESZ – existujúce zálohovacie riešenie je z pohľadu zálohovacích mechanizmov decentralizované vzhľadom na rôznorodosť platforiem použitých v riešení. Záložné kópie dát sú vytvárané na niekoľkých úrovniach:

1. synchrónna replikácia údajov v rámci primárnej lokality
2. záloha údajov na diskovom systéme v rámci primárnej lokality
3. záloha dát na pásky v rámci primárnej lokality
4. presun pások do zabezpečených priestorov mimo primárnu lokalitu

Technológia ukladania záloh na pásky neumožňuje z pohľadu obnovy služieb NZIS dosiahnuť akceptovateľné časy. Presun záložných kópii dát mimo produkčnú lokalitu sa uskutočňuje neautomatizovaným spôsobom, čo zvyšuje nároky na personálne zabezpečenie a komplikuje pravidelnú verifikáciu konzistencie dát uložených na záložných kópiách mimo produkčnej lokality a taktiež komplikuje pravidelné testy obnoviteľnosti služieb NZIS zo záložných kópií uložených mimo produkčnú lokalitu. Vzhľadom na vyššie uvedené skutočnosti a absenciu záložnej lokality je možné hodnotiť aktuálny stav za nedostatočný.

Vzhľadom na vyššie uvedené skutočnosti a absenciu:

- metodík riadenia prevádzky
- nastavenia IT procesov
- nasadenia informačných systémov pre podporu prevádzky
- záložnej lokality
- personálneho zabezpečenia prevádzky

je možné hodnotiť aktuálny stav pre použitie v rámci projektu NZIS za nedostatočný.

Priestor pre sumárny obrázok / graf / diagram, nepovinná informácia.

Ďalšie informácie
(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)

Riziká **Spresnenie identifikovaných rizík:** *R_2, R_3*

- R_2 Prevádzka nie je dostatočne pokrytá internými pracovníkmi, čo brzdí operatívu aj rozvojové projekty
- R_3 Nedostatočná forma dodávateľskej podpory môže mať za následok dlhšie odstraňovanie problémov

Prílohy	**Diagramy, modely, obrázky v plnom rozlíšení**
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	*Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*

Alternatívne riešenia

V nasledujúcom texte sú porovnávané navrhované alternatívy a následné vstupné kritéria do multikriteriálnej analýzy, ktoré boli stanovené na základe identifikovaných problémov a príležitostí na zlepšenia. Do úvahy boli brané nasledovné ciele, požiadavky a obmedzenia:

Cieľ	**Požiadavka/KPI**	**Obmedzenie**
Prevádzkovo stabilná, bezpečná a cenovo udržateľná infraštruktúra	Zlepšenie dostupnosti	Zastaralá infraštruktúra ezdravie, znižuje SLA. Nedostatočná kapacita brzdí zvyšovanie pokrytia poskytovaných el. služieb.
BCM a DRP v súlade s legislatívnymi požiadavkami	Znížené prevádzkové náklady	
Dynamicky poskytovaný výkon	Podiel riešení s využitím IaaS služieb	Potreba reagovať na dynamické výkyvy pri poskytovaní el. služieb ezdravie. Peeky ako napr. epidémie
Aktualizácia platforiem a zavedenie pay-per-use tam kde to bude možné	Podiel riešení s využitím PaaS služieb	Problematická migrácia na novšie verzie a kapacitné obmedzenia licencovaných platforiem
Nastavenie nových architektonických princípov v zmysle moderných trendov	Podiel uplatnených nových architektonických princípov	Zastaralé architektonické princípy ezdravie zužujú a komplikujú technologický priestor na možné riešenia modernizácie
Zachovanie bezpečnostných požiadaviek v adekvátnej úrovni k súčasnému stavu	Podiel uplatnených súčasných bezpečnostných požiadaviek	Zamedziť kompromitácii ezdravia

Zavedenie modernizovaného systému monitorovania a vyhodnocovania bezpečnostných incidentov v súlade s novými architektonickými princípmi. Zároveň sa integrovať na centrálny CSIRT	% uzavretých bezpečnostných. incidentov v stanovenom SLA čase	Monitoring a vyhodnocovanie bezpečnostných incidentov je zastaralý a prevádzkovo náročný
Zavedenie modernizovaného systému monitorovania a vyhodnocovania prevádzkových incidentov s súlade s novými architektonickými princípmi.	% uzavretých incidentov v stanovenom SLA čase	Monitoring a vyhodnocovanie prevádzkových incidentov je zastaralý a prevádzkovo náročný
Zjednodušenie, sprehľadnenie a zrýchlenie zložitých prevádzkových postupov	Skrátenie času nasadzovania	Zmenu nevieme nasadiť do 1 hodiny, ale trvá to niekoľko dní. V prípade že ide o nadsadenie kritických zmien, tak je to problém - súvisiaci s SLA služieb
Zjednodušenie, sprehľadnenie a zrýchlenie komplikovaného release managementu	Celkový čas riešenia incidentu od identifikácie po nasadenia na PROD	Pre každé prostredie je dedikovaný release management, z dôvodu že ostatné prostredia okrem prod sú značne oklieštené z finančných dôvodov (chýbajúce HA, balancery, špecifické bezpečnostné mechanizmy, ...)

Nulový variant – ponechanie súčasného stavu

Alternatíva – „Preferovaný variant"

Súhrnný popis

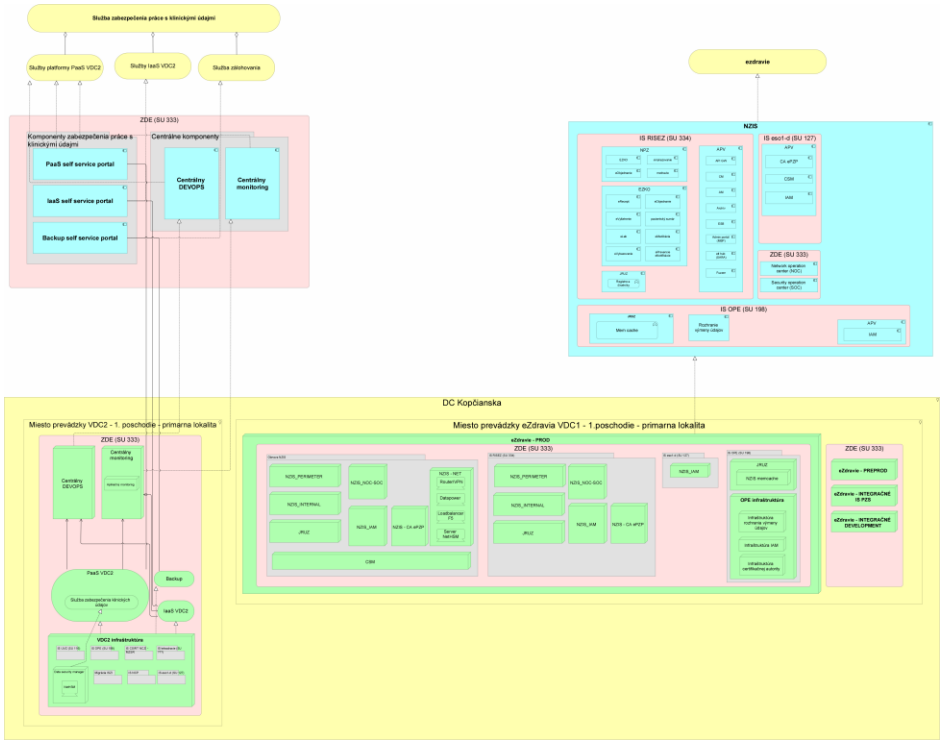
Táto alternatíva sa zaoberá stabilizáciou riešenia ezdravie, a poskytnutím prostredia pre riešenie rozvojových projektov rezortu zdravotníctva. Obsahuje nasledujúce výstupy:

Pre ezdravie

- Vybudovanie bezpečnej a kapacitne dostatočnej infraštruktúry
- Vybudovanie novej systémovej architektúry
- Vybudovanie nového monitoringu bezpečnostných incidentov
- Vybudovanie nového monitoringu prevádzkových incidentov
- Zachovanie bezpečnostných princípov v adekvátnej úrovni k súčasnému stavu
- Posúdenie systémovej architektúry
- Nový model hrozieb
- Návrh komplementárnych bezpečnostných princípov
- Návrh novej bezpečnosti
- SDL v.2
- Aktualizovaný bezpečnostný projekt
- Migrácia systému ezdravie do nového prostredia
- Zjednodušenie, sprehľadnenie a zrýchlenie zložitých prevádzkových postupov
- Zjednodušenie, sprehľadnenie a zrýchlenie komplikovaného release managementu

Pre nové rozvojové projekty rezortu zdravotníctva

- Vybudovanie bezpečnej a kapacitne dostatočnej infraštruktúry
- Dynamicky poskytovaná infraštruktúra a platformy
- Vybudovanie novej systémovej architektúry
- Zavedenie služieb zálohovania a obnovy zálohy.
- Automatizovaný DEVOPS
- Zachovanie bezpečnostných princípov v adekvátnej úrovni k súčasnému stavu
- Aktualizovaný bezpečnostný projekt
- Nezávislý audit bezpečnosti



Ďalšie informácie
(Max. 800 znakov)

Dôvod zamietnutia, alebo výberu riešenia (Max. 400 znakov)

Alternatíva – „Maximalistický variant"

Súhrnný popis

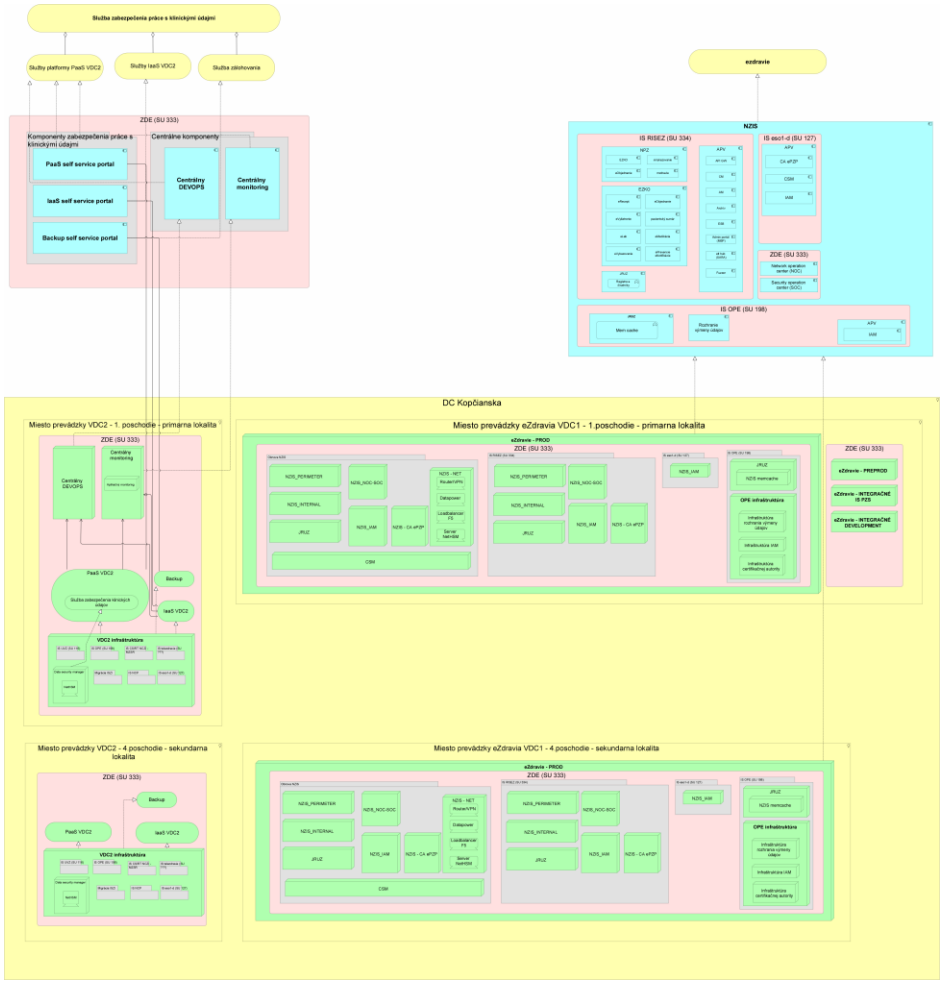
Táto alternatíva sa zaoberá stabilizáciou riešenia ezdravie, poskytnutím prostredia pre riešenie rozvojových projektov rezortu zdravotníctva a umiestenie ďalších IS v rámci rezortu zdravotníctva, alebo zapojených organizácii v systéme ezdravie. Obsahuje nasledujúce výstupy:

Pre ezdravie

- Vybudovanie bezpečnej a kapacitne dostatočnej infraštruktúry
- Vybudovanie novej systémovej architektúry
- Vybudovanie záložného riešenia, príprava DRP a BCM postupov a ich aplikácia v režime active-active.
- Vybudovanie nového monitoringu bezpečnostných incidentov
- Vybudovanie nového monitoringu prevádzkových incidentov
- Zachovanie bezpečnostných princípov v adekvátnej úrovni k súčasnému stavu
- Posúdenie systémovej architektúry
- Nový model hrozieb
- Návrh komplementárnych bezpečnostných princípov
- Návrh novej bezpečnosti
- SDL v.2
- Aktualizovaný bezpečnostný projekt
- Zjednodušenie, sprehľadnenie a zrýchlenie zložitých prevádzkových postupov
- Zjednodušenie, sprehľadnenie a zrýchlenie komplikovaného release managementu
- Migrácia systému ezdravie do nového prostredia

Pre nové rozvojové projekty rezortu zdravotníctva

- Vybudovanie bezpečnej a kapacitne dostatočnej infraštruktúry
- Dynamicky poskytovaná infraštruktúra a platformy
- Vybudovanie novej systémovej architektúry
- Vybudovanie záložného riešenia, príprava DRP a BCM postupov a ich aplikácia.
- Zavedenie služieb zálohovania a obnovy zálohy.
- Automatizovaný DEVOPS
- Zachovanie bezpečnostných princípov v adekvátnej úrovni k súčasnému stavu
- Aktualizovaný bezpečnostný projekt
- Nezávislý audit bezpečnosti



Ďalšie informácie
(Max. 800 znakov)

Dôvod zamietnutia, alebo výberu riešenia (Max. 400 znakov)

Multikriteriálna analýza

Zúženie uvedených alternatív riešenia prebieha prostredníctvom multikriteriálnej analýzy (MCA) zostavenej na základe kapitoly Motivácia, ktorá obsahuje ciele stakeholderov, ich požiadavky a obmedzenia pre dosiahnutie uvedeného cieľa.

Aktér	**Kritérium**	**KO**
	Bezpečná a kapacitne dostatočná infraštruktúra	Áno
	Dynamicky poskytovaný výkon	Nie
NCZI	Pay-per-use	Nie
	Nové architektonické princípy v zmysle moderných trendov	Nie
	BCM a DRP v súlade s legislatívnymi požiadavkami	Nie

	Zachovanie bezpečnostných požiadaviek v adekvátnej úrovni k súčasnému stavu	Áno
	Systém monitorovania a vyhodnocovania bezpečnostných incidentov	Nie
	Systém monitorovania a vyhodnocovania prevádzkových incidentov	Nie
	Zjednodušenie, sprehľadnenie a zrýchlenie zložitých prevádzkových postupov	Nie
	Zjednodušenie, sprehľadnenie a zrýchlenie komplikovaného release managementu	Nie
	Produkčné prostredie v súlade s legislatívnymi požiadavkami zákona č. 153/2013 Z. z. (NZIS)	Áno
	Bezpečná a kapacitne dostatočná infraštruktúra	Áno
	Dynamicky poskytovaný výkon	Áno
	Pay-per-use	Áno
	Nové architektonické princípy v zmysle moderných trendov	Nie
	BCM a DRP v súlade s legislatívnymi požiadavkami	Nie
Organizácie MZSR	Systém monitorovania a vyhodnocovania bezpečnostných incidentov	Nie
	Systém monitorovania a vyhodnocovania prevádzkových incidentov	Nie
	Zjednodušenie, sprehľadnenie a zrýchlenie zložitých prevádzkových postupov	Nie
	Zjednodušenie, sprehľadnenie a zrýchlenie komplikovaného release managementu	Nie
	Produkčné prostredie v súlade s legislatívnymi požiadavkami zákona 153/2013 Z. z. (NZIS)	Áno

Nulový variant

Aktér	Kritérium	Plnenie	Vysvetlenie
NCZI	Bezpečná a kapacitne dostatočná infraštruktúra	Čiastočne	Zabezpečené čiastočne v rámci havarijných opráv.
	Dynamicky poskytovaný výkon	Nie	Pre prácu s klinickými údajmi, takéto riešenie nie je k dispozícii (ani v rámci vládneho cloudu).
	Pay-per-use	Nie	Pre prácu s klinickými údajmi, takéto riešenie nie je k dispozícii (ani v rámci vládneho cloudu).
	Nové architektonické princípy v zmysle moderných trendov	Nie	Ponechanie súčasného stavu nevytvára priestor na architektonický re dizajn ezdravia.

	BCM a DRP v súlade s legislatívnymi požiadavkami	Nie	BCM a DRP v obmedzenom režime – jeden site.
	Zachovanie bezpečnostných požiadaviek v adekvátnej úrovni k súčasnému stavu	Čiastočne	Požiadavka splnená čiastočne pretože výrobcom už nepodporovaná infraštruktúra (EOL) tiež predstavuje bezpečnostné riziko.
	Systém monitorovania a vyhodnocovania bezpečnostných incidentov	Nie	Monitoring a vyhodnocovanie bezpečnostných incidentov je zastaralý a prevádzkovo náročný
	Systém monitorovania a vyhodnocovania prevádzkových incidentov	Nie	Monitoring a vyhodnocovanie prevádzkových incidentov je zastaralý a prevádzkovo náročný
	Zjednodušenie, sprehľadnenie a zrýchlenie zložitých prevádzkových postupov	Nie	Ponechanie súčasného stavu prináša iba zanedbateľný priestor na zlepšenie v rámci stanovených KPI
	Zjednodušenie, sprehľadnenie a zrýchlenie komplikovaného release managementu	Nie	Ponechanie súčasného stavu prináša iba zanedbateľný priestor na zlepšenie v rámci stanovených KPI
	Bezpečná a kapacitne dostatočná infraštruktúra	Nie	Pre prácu s klinickými údajmi, takéto riešenie nie je k dispozícii (ani v rámci vládneho cloudu).
	Dynamicky poskytovaný výkon	Nie	Pre prácu s klinickými údajmi, takéto riešenie nie je k dispozícii (ani v rámci vládneho cloudu).
	Pay-per-use	Nie	Pre prácu s klinickými údajmi, takéto riešenie nie je k dispozícii (ani v rámci vládneho cloudu).
Organizácie MZSR	Nové architektonické princípy v zmysle moderných trendov	Nie	Pre prácu s klinickými údajmi, takéto riešenie nie je k dispozícii (ani v rámci vládneho cloudu).
	BCM a DRP v súlade s legislatívnymi požiadavkami	Nie	Pre prácu s klinickými údajmi, takéto riešenie nie je k dispozícii (ani v rámci vládneho cloudu).
	Systém monitorovania a vyhodnocovania bezpečnostných incidentov	Nie	Pre prácu s klinickými údajmi, takéto riešenie nie je k dispozícii (ani v rámci vládneho cloudu).
	Systém monitorovania a vyhodnocovania prevádzkových incidentov	Nie	Pre prácu s klinickými údajmi, takéto riešenie nie je k dispozícii (ani v rámci vládneho cloudu).

	Zjednodušenie, sprehľadnenie a zrýchlenie zložitých prevádzkových postupov	Nie	Pre prácu s klinickými údajmi, takéto riešenie nie je k dispozícii (ani v rámci vládneho cloudu).
	Zjednodušenie, sprehľadnenie a zrýchlenie komplikovaného release managementu	Nie	Pre prácu s klinickými údajmi, takéto riešenie nie je k dispozícii (ani v rámci vládneho cloudu).

Preferovaný variant

Aktér	Kritérium	Plnenie	Vysvetlenie
NCZI	Bezpečná a kapacitne dostatočná infraštruktúra	Áno	Riešenie VDC1 a VDC2 zabezpečuje plnenie tohto kritéria
	Dynamicky poskytovaný výkon	Nie	Riešenie VDC2 zabezpečuje plnenie tohto kritéria
	Pay-per-use	Nie	Riešenie VDC2 zabezpečuje plnenie tohto kritéria
	Nové architektonické princípy v zmysle moderných trendov	Áno	V rámci aktivít projektu bude pripravená nová systémová architektúra aplikovaná pri migrácii ezdravia
	BCM a DRP v súlade s legislatívnymi požiadavkami	Čiastočne	Riešenie VDC1 a VDC2 zabezpečuje plnenie tohto kritéria celkových zlepšením dostupnosti avšak bez záložnej lokality
	Zachovanie bezpečnostných požiadaviek v adekvátnej úrovni k súčasnému stavu	Áno	Požiadavka splnená obnovou a modernizáciou bezpečnostnej infraštruktúry a spracovaním nového bezp. projektu.
	Systém monitorovania a vyhodnocovania bezpečnostných incidentov	Áno	Požiadavka naplnená novým systémom monitorovania a vyhodnocovania bezp. incidentov.
	Systém monitorovania a vyhodnocovania prevádzkových incidentov	Áno	Požiadavka naplnená novým systémom monitorovania a vyhodnocovania prevádzkových incidentov.
	Zjednodušenie, sprehľadnenie a zrýchlenie zložitých prevádzkových postupov	Áno	Kritérium splnené novou systémovou architektúrou v súlade s DEVOPS princípmi.
	Zjednodušenie, sprehľadnenie a zrýchlenie komplikovaného release managementu	Áno	Kritérium splnené novou systémovou architektúrou v súlade s DEVOPS princípmi.

	Bezpečná a kapacitne dostatočná infraštruktúra	Áno	Riešenie VDC2 zabezpečuje plnenie tohto kritéria
	Dynamicky poskytovaný výkon	Áno	Riešenie VDC2 zabezpečuje plnenie tohto kritéria
	Pay-per-use	Áno	Riešenie VDC2 zabezpečuje plnenie tohto kritéria
	Nové architektonické princípy v zmysle moderných trendov	Áno	V rámci aktivít projektu bude pripravená nová systémová architektúra aplikovaná pre ostatné organizácie MZSR
	BCM a DRP v súlade s legislatívnymi požiadavkami	Čiastočne	Riešenie VDC2 zabezpečuje plnenie tohto kritéria celkových zlepšením dostupnosti avšak bez záložnej lokality
Organizácie MZSR	Systém monitorovania a vyhodnocovania bezpečnostných incidentov	Áno	Požiadavka naplnená novým systémom monitorovania a vyhodnocovania bezp. incidentov v multi-tenant režime aj pre ostatné organizácie rezortu zdravotníctva.
	Systém monitorovania a vyhodnocovania prevádzkových incidentov	Áno	Požiadavka naplnená novým systémom monitorovania a vyhodnocovania prevádzkových incidentov v multi-tenant režime aj pre ostatné organizácie rezortu zdravotníctva.
	Zjednodušenie, sprehľadnenie a zrýchlenie zložitých prevádzkových postupov	Áno	Kritérium splnené novou systémovou architektúrou v súlade s DEVOPS princípmi.
	Zjednodušenie, sprehľadnenie a zrýchlenie komplikovaného release managementu	Áno	Kritérium splnené novou systémovou architektúrou v súlade s DEVOPS princípmi.

Maximalistický variant

Aktér	Kritérium	Plnenie	Vysvetlenie
	Bezpečná a kapacitne dostatočná infraštruktúra	Áno	Riešenie VDC1 a VDC2 zabezpečuje plnenie tohto kritéria
	Dynamicky poskytovaný výkon	Nie	Riešenie VDC2 zabezpečuje plnenie tohto kritéria
NCZI	Pay-per-use	Nie	Riešenie VDC2 zabezpečuje plnenie tohto kritéria
	Nové architektonické princípy v zmysle moderných trendov	Áno	V rámci aktivít projektu bude pripravená nová systémová architektúra aplikovaná pri migrácii ezdravia

	BCM a DRP v súlade s legislatívnymi požiadavkami	Áno	Riešenie VDC1 a VDC2 zabezpečuje plnenie tohto kritéria
	Zachovanie bezpečnostných požiadaviek v adekvátnej úrovni k súčasnému stavu	Áno	Požiadavka splnená obnovou a modernizáciou bezpečnostnej infraštruktúry a spracovaním nového bezp. projektu.
	Systém monitorovania a vyhodnocovania bezpečnostných incidentov	Áno	Požiadavka naplnená novým systémom monitorovania a vyhodnocovania bezp. incidentov.
	Systém monitorovania a vyhodnocovania prevádzkových incidentov	Áno	Požiadavka naplnená novým systémom monitorovania a vyhodnocovania prevádzkových incidentov.
	Zjednodušenie, sprehľadnenie a zrýchlenie zložitých prevádzkových postupov	Áno	Kritérium splnené novou systémovou architektúrou v súlade s DEVOPS princípmi.
	Zjednodušenie, sprehľadnenie a zrýchlenie komplikovaného release managementu	Áno	Kritérium splnené novou systémovou architektúrou v súlade s DEVOPS princípmi.
	Bezpečná a kapacitne dostatočná infraštruktúra	Áno	Riešenie VDC2 zabezpečuje plnenie tohto kritéria
	Dynamicky poskytovaný výkon	Áno	Riešenie VDC2 zabezpečuje plnenie tohto kritéria
	Pay-per-use	Áno	Riešenie VDC2 zabezpečuje plnenie tohto kritéria
	Nové architektonické princípy v zmysle moderných trendov	Áno	V rámci aktivít projektu bude pripravená nová systémová architektúra aplikovaná pre ostatné organizácie MZSR
Organizácie MZSR	BCM a DRP v súlade s legislatívnymi požiadavkami	Áno	Riešenie VDC2 zabezpečuje plnenie tohto kritéria
	Systém monitorovania a vyhodnocovania bezpečnostných incidentov	Áno	Požiadavka naplnená novým systémom monitorovania a vyhodnocovania bezp. incidentov v multi-tenant režime aj pre ostatné organizácie rezortu zdravotníctva.
	Systém monitorovania a vyhodnocovania prevádzkových incidentov	Áno	Požiadavka naplnená novým systémom monitorovania a vyhodnocovania prevádzkových incidentov v multi-tenant režime aj pre ostatné organizácie rezortu zdravotníctva.

Zjednodušenie, sprehľadnenie a zrýchlenie zložitých prevádzkových postupov	Áno	Kritérium splnené novou systémovou architektúrou v súlade s DEVOPS princípmi.
Zjednodušenie, sprehľadnenie a zrýchlenie komplikovaného release managementu	Áno	Kritérium splnené novou systémovou architektúrou v súlade s DEVOPS princípmi.

Nulový variant – „ponechanie súčasného stavu"

Súhrnný popis

Výhody

- Úspora investičných EŠIF prostriedkov

Nevýhody

- Zastaralá infraštruktúra - opravy budú financované zo štátneho rozpočtu
- Zastaralý model hrozieb
- Prevádzkové náklady s tendenciou nárastu
- Zastavené resp. výrazne posunuté ďalšie rozvojové aktivity ezdravia ako aj ďalších projektov (vid. Popis budúceho stavu – Architektúra).

Nesplnenie legislatívnych požiadaviek (vid. Popis budúceho stavu - Legislatíva)

V prípade tohto variantu je na jednej strane síce zrejmá úspora investičných EŠIF prostriedkov, na druhej strane však bude prevádzka ponechaná v hraničnej situácii poskytovania služieb na výrazne zastaralej infraštruktúre. Čo bude mať za následok čoraz zásadnejšie prevádzkové problémy, ktoré budú vyvolávať problémy pri výkonoch jednotlivých PZS

Preferovaný variant

Súhrnný popis

Výhody

- Obnova a modernizácia infraštruktúry ezdravia
- Kapacitný priestor pre nové rozvojové aktivity v rámci ezdravia
- Kapacitný priestor pre nové rozvojové aktivity v rámci rezortu zdravotníctva s zohľadnením bezpečnostných požiadaviek pre prácu s klinickými údajmi
- Optimalizácia prevádzkových nákladov

Nevýhody

Z pohľadu porovnania jednotlivých alternatív, ani táto alternatíva úplne nerieši záložnú infraštruktúru, ktorý by zohľadňovala všetkých bezpečnostné požiadavky a požiadavky na dostupnosť.

Tento variant predstavuje naplnenie všetkých KO kritérií a výhodnejší pomer prínosov a nákladov, aj napriek tomu, že definitívne nerieši vybudovanie BCM a DRP.

Maximalistický variant

Súhrnný popis

Výhody

- Obnova a modernizácia infraštruktúry ezdravia
- Kapacitný priestor pre nové rozvojové aktivity v rámci ezdravia
- Kapacitný priestor pre nové rozvojové aktivity v rámci rezortu zdravotníctva s zohľadnením bezpečnostných požiadaviek pre prácu s klinickými údajmi
- Optimalizácia prevádzkových nákladov
- Vyššie dosiahnuteľné KPI v porovnaní s preferovanou variantou
- Záložná lokalita – pri zohľadnení všetkých bezpečnostných požiadaviek a požiadaviek na dostupnosť

Nevýhody

Vysoké náklady

Aj napriek splneniu všetkých kritérií je táto alternatíva zamietnutá z dôvodu vysokých nákladov, resp. nižšiemu BCR ako preferovaný variant. Z strednodobom časovom horizonte, je však odporúčané aby celková architektúra z podhľadu dostupnosti ezdravia bola dobudovaná práve do podoby, ktorú reprezentuje tento variant.

Vyhodnotenie

Žiadne z kritérií nebolo určené ako KO, a preto bola pre každú alternatívu spracovaná CBA s nasledujúcimi výsledkami

Alternatívy	Celkové kapitálové výdavky projektu EUR s DPH	Čistá súčasná ekonomická hodnota (ENPV) EUR bez DPH	Rok návratu investície (PBP)	BCR (pomer prínosov a nákladov)
Alternatíva – „Preferovaný variant"	48 109 246	40 070 968	5. rok	4,1
Alternatíva – „Maximalistický variant"	80 544 678	55 476 951	6. rok	2,94

Na základe vyššie uvedeného bola zvolená alternatíva s najlepším pomerom prínosov a nákladov – ďalej nazývaná Preferovaný variant

Popis budúceho stavu

Legislatíva

Tabuľka 10 Legislatíva - budúci stav

Súhrnný popis

Riešenie musí zabezpečiť súlad s právnymi predpismi uvedenými v kapitole Legislatíva - súčasný stav a ich aktuálne platným znením počas realizácie projektu ZDE. Keďže projekt ZDE je infraštruktúrny a nerieši procesné zmeny, nie sú implicitne potrebné legislatívne úpravy. Počas projektu bude nutné sledovať a pripomienkovať legislatívne normy, ktoré sa projektu ZDE týkajú, tak aby nevznikli legislatívne prekážky pri realizácii projektu ZDE.

Priestor pre sumárny obrázok / graf / diagram, nepovinná informácia.

Ďalšie informácie
(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)

Kritéria kvality

Spresnenie kritérií kvality: *Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.*

Stručná charakteristika požadovanej kvality (Max. 400 znakov)

Riziká

Spresnenie identifikovaných rizík: *R_4*

- R_4 Politické riziko pri zmene vlády

Prílohy	**Diagramy, modely, obrázky v plnom rozlíšení**
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	*Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*

Architektúra

V tejto časti je popísaná architektúra vybraného riešenia.

Všetky mená uvedených produktov sú pre VDC2 ilustratívne, použité za účelom lepšieho popisu, čo má dané riešenie spĺňať. Pre VDC1 vychádza návrh z existujúceho dizajnu riešenia pri zachovaní výkonových parametrov riešenia.

Biznis architektúra

Tabuľka 11 Biznis architektúra – budúci stav

Súhrnný popis

Prostredie pre nové rozvojové projekty rezortu zdravotníctva a ďalšie zapojené organizácie zdravotníctva (VDC2)

Zavedenie PaaS platformy umožní kontinuálnu podporu a rozvoj IT prístupu v nasledovných oblastiach:

- Architektúry – podpora prechodu od monolitických aplikácií k mikroslužbám a kompozitným aplikáciám
- Metodológie – od lineárnych-sekvenčných k Agilným, DevOps, CI-CD postupom
- Technológií – od Aplikačných serverov na hostoch k PaaS platforme, kontajnerom, hybridným cloudom
- Nasadzovania – podpora prechodu do produkcie v ľubovoľnom čase
- Monitoringu a správy – od veľa rôznych nástrojov, k cielenej automatizácii, správe služieb a nie serverov

Služby poskytované natívnou platformou PaaS, z hľadiska ich využitia musia spĺňať požiadavky pre podporu aplikácií viacerých úrovní dostupnosti. S ohľadom na kritickosť aplikácií. Je teda požadované aby služby nasadené na platformu, poskytovali na základe SLA viac modelov - variantov jednotlivých služieb. V prostredí PaaS sa tieto modely nazývajú aj Plány služby PaaS. Minimálna požiadavka je na služby PaaS je pre každú služby (ak je to samozrejme realizovateľné) poskytnúť 3 plány (úrovne služby). Z pohľadu označovania je vhodné plány (úrovne služieb) nazývať napríklad:

- Bronze
- Silver
- Gold

Plán služby Bronze

Bronze predstavuje najnižšiu úroveň z pohľadu dostupnosti a je charakterizovaný jedno uzlovou-nódovou implementáciou, kde služba beží na jednom výpočtovom uzle a predstavuje SPOF (single point of failure) z pohľadu SLA, kde RTO (čas obnovy – recovery time) je závislý od rýchlosti robnovy zálohy. RPO (bod ku ktorému je obnova - recovery point) je závislý od nastavenia zálohovania.

Plán služby Silver

Silver predstavuje zvýšenú úroveň z pohľadu dostupnosti a je charakterizovaný viac nódovým nasadením služby (za pohľadu optimálnej dostupnosti 3 a viac nódov), pričom samotná implementácia môže byť realizovaná replikáciami, HA A-A, HA A-P klastrami, a podobne. Z pohľadu nasadenia je realizácia služby v rámci jednej geografickej lokality. Dostupnosť je

vysoká, ale nevýhodou je práve limitácia v rámci jednej lokality, teda je potrebné riešiť DR a doba obnovy ako aj bod obnovy v prípade havárie lokality závisí do zálohovania.

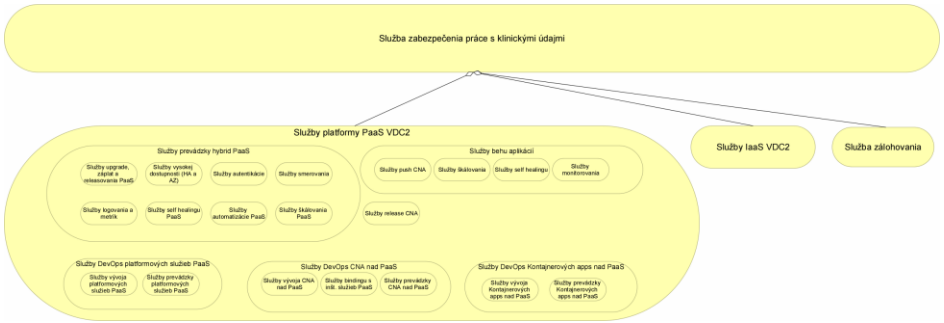
Plán služby Gold

Gold predstavuje najvyššiu úroveň z pohľadu dostupnosti a je charakterizovaný viac nódovým nasadením služby (za pohľadu optimálnej dostupnosti 3 a viac nódov), pričom samotná implementácia môže byť realizovaná replikáciami, HA A-A, HA A-P klastrami, a podobne. z pohľadu nasadenia je služba rozprestrená na viac geografických lokalít. Týmto sa odstraňuje nevýhoda plánu služby Silver.

Aby sa docielili čo najvyššie prínosy plynúce z použitia cloudových technológií, je architektúra navrhnutá modulárne s unifikovaným stavebným blokom. Pričom v prípade potreby rozširovania sa dajú tieto bloky dokupovať podľa potreby. Licenčný model cloudových technológii pre IaaS počíta s tzv. „service provider“ licenčným modelom, platilo by sa iba za skutočne nasadené zdroje.

V rámci tejto štúdie uskutočniteľnosti sa počíta s blokmi, ktoré sa zakúpia počas trvania projektu, tak aby reflektovali požadovanú kapacitu pripravovaných projektov rezortu zdravotníctva.

Služby platformy PaaS



Sú očakávané nasledovne služby PaaS platformy:

- **Služby prevádzky hybrid PaaS**
  - Služby smerovania
  - Služby autentikácie
  - Služby vysokej dostupnosti (HA a AZ)
  - Služby škálovania PaaS
  - Služby upgrade, záplat a releasovania PaaS
  - Služby automatizácie PaaS
  - Služby logovania a metrík

    - Služby self healingu PaaS
    - Služby automatizácie PaaS

- **Služby životného cyklu platformových služieb**
    - Služby DevOps platformových služieb PaaS
        - Služby vývoja platformových služieb PaaS
        - Služby prevádzky platformových služieb PaaS

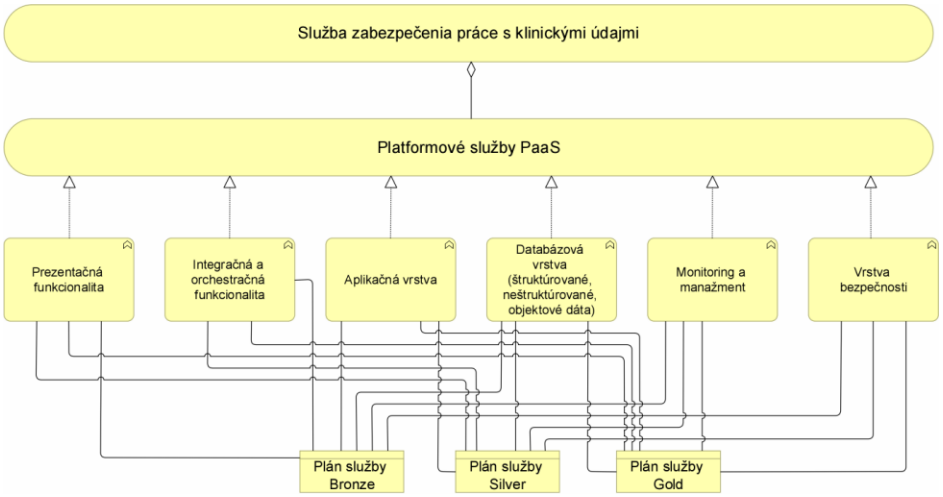
- **Služby životného cyklu aplikácií a služieb CNA**
    - Služby DevOps CNA nad PaaS
        - Služby vývoja CNA nad PaaS
        - Služby prevádzky CNA nad PaaS
        - Služby bindingu s inšt. služieb PaaS

- **Služby životného cyklu kontajnerových app**
    - Služby DevOps Kontajnerových apps nad PaaS
        - Služby vývoja Kontajnerových apps nad PaaS
        - Služby prevádzky Kontajnerových apps nad PaaS

- **Služby behu aplikácií**
    - Služby push CNA
    - Služby škálovania
    - Služby self healingu
    - Služby monitorovania

- **Služby releasovania**

Platformové služby PaaS



Predstavujú základnú sadu služieb, ktoré budú v rámci PaaS platformy pripravené, t.j. v prípade CF bude pripravený service adaptér, služba bude otestovaná a bude zaradená do Service registry.

Prezentačná funkcionalita

Služby	Bronze	Silver	Gold
NGINX	X	X	

Integračná a orchestračná funkcionalita

Služby	Bronze	Silver	Gold
RabbitMQ	X	X	
Apache Kafka	X	X	
Kong	X	X	X

Aplikačná vrstva

Služby	Bronze	Silver	Gold
Apache Tomcat	X	X	
Steeltoe (.NET core, .NET framework)	X	X	

Databázová vrstva (štruktúrované, neštruktúrované, objektové dáta)

Služby	Bronze	Silver	Gold
Mysql	X	X	X
Microsoft SQL	X	X	X
Postresql	X	X	X
MongoDB	X	X	
Redis	X	X	
NFS	X	X	X
S3	X	X	

Monitoring a manažment

Služby	Bronze	Silver	Gold
Gitlab	X	X	X
Elasticsearch	X	X	
Kibana	X	X	

Vrstva bezpečnosti

Služby	Bronze	Silver	Gold
Midpoint	X	X	
Vormetrix transparent encryption for PCF	X	X	X
Thales eSecurity (CipherTrust Cloud Key Manager)	X	X	X

Priestor pre sumárny obrázok: ArchiMate štandardný viewpoint – „Product viewpoint", „Business Process Viewpoint"

Ďalšie informácie
(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)

Kritéria kvality

Spresnenie kritérií kvality: *R_6*

- R_6 Procesy devops sa nepodarí pretaviť do praxe

Riziká

Spresnenie identifikovaných rizík: *Odkazy na relevantné identifikátory rizík v prílohe Riziká.*

Stručná charakteristika identifikovaných rizík (Max. 400 znakov)

Prílohy

Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.

Diagramy, modely, obrázky v plnom rozlíšení

Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

Architektúra informačných systémov

Tabuľka 12 Architektúra informačných systémov - budúci stav

Súhrnný popis

Prostredie pre nové rozvojové projekty rezortu zdravotníctva a ďalšie zapojené organizácie zdravotníctva (VDC2)

PaaS

Pre toto prostredie umažujeme s Cloud natívnou PaaS platformou, ktorá je podporovaná infraštruktúrnou vrstvou (vid. IaaS) a podporuje aplikačnú a servisnú vrstvu. Cloud-natívna platforma poskytne prostredie pre projekty rezortu zdravotníctva a ďalšie zapojené organizácie zdravotníctva s pridanou hodnotu.

Kľúčové požiadavky Cloud natívnej PaaS platformy pre organizácie v rámci rezortu sú nasledovné:

- Služby ako abstrakcia infraštruktúry a middleware, ktoré sú poskytnuté samoobslužným mechanizmom. Takto sa odstráni réžia určená na správu infraštruktúrnych vrstiev, čo výrazne zníži čas vývoja a nasadenia aplikácií.
- Kontajnery a podpora použitia kontajnerových snímok a podpora automatickej kontajnerizácie nasadených artefaktov aplikácií. Táto vlastnosť umožní využívať už vytvorené aplikácie kontajnerového typu a vytvárať nové. Automatická kontajnerizácia aplikácií prinesie tiež zvýšenie produktivity a prevádzkové výhody, pretože prevádzkovaný kontajner zo snímky je zvyčajne zostavený zo známych a preverených komponentov platformy, pričom väčšinou len zdrojový kód aplikácie podlieha skenovaniu na zraniteľnosť.
- Agilita a automatizácia – PaaS platformu musí byť možné využiť ako súčasť DevOps, CI/ CD procesov vytvorených pre nasadenie prevádzkových a vývojových prostredí a aj samotných služieb. Podporí sa tak kľúčová požiadavka na agilitu vytvárania aplikácií a dodávku hotových riešení v požadovanom čase.
- Platforma PaaS musí podporiť kultúrny posun k DevOps metodológii vývoja a prevádzky cloud aplikácií
- Podpora mikroslužieb - PaaS platforma podporí mikroslužby poskytnutím softvérových mechanizmov pre integráciu a koordináciu voľne prepojených služieb.
- Podpora cloud-natívnych aplikácií CNA – PaaS platforma musí poskytnúť „kontrakty“ (rozhrania) pre aplikácie, ktoré sú vyvíjane nad platformou. Architektonický štýl známy CNA bol vytvorený pre popis konštrukciu aplikácií napísaných špeciálne pre spustenie v prostredí cloudu. Tieto aplikácie sa musia vyhnúť niektorým z anti-vzorov, ktoré boli stanovené v klient-server ére. Definície Dvanásť Faktorovej Aplikácie vysvetľujú princípy, na ktorých sú a budú budované cloud-natívne aplikácie, čo možno považovať za kontrakt medzi aplikáciou a cloud-natívnou platformou.
- PaaS platforma musí mať unifikované riešenia pre tzv boiler-plate responsibilities (aktivity ktoré musia byt realizované pre každú aplikáciu rovnako)
- PaaS platforma musí byť infraštruktúrne agnostická, čo je realizované cloud operačným systémom, ktorý využíva cloudové zdroje a tie sú skryté koncovému požívateľovi. Platforma abstrahuje infraštruktúrne výpočtové zdroje (virtuálne úložisko, siete, RAM a CPU).
- Musí umožniť nasadiť predkompilovaný kontajnerový image-obraz, alebo aplikačný artefakt (zdrojový kód alebo binárne súbory), ktoré doteraz neboli v kontajneroch.

- Zavedie samoobslužný prístup, odstráni potenciálne zdĺhavé oneskorenie medzi tímami. Napríklad schopnosť nasadenia aplikácií, poskytovanie aplikácií a väzba na služby, škálovanie , monitoring a upgrade.
- Platforma PaaS musí poskytovať responzívnu IT prevádzku s plnou viditeľnosť a kontrolou nad životným cyklom aplikácií, ich provisioningom, nasadením, aktualizáciou a bezpečnosťou.
- Platforma poskytne elasticitu a samo-liečenie na základe spätnej väzby. Pružnosť je dôležitá, ale často nákladná súčasť zaistenia kontinuity prevádzky. Platforma musí automatizovať obnovu „spadnutých“ aplikácií, komponentov a procesov. Takýto self-healing odstráni záťaž pre obnovu zo strany prevádzkovateľa PaaS platformy, čo zaisťuje rýchlosť zotavenia.
- Poskytne náhľad cez agregované logy a metriky do aplikácií a platformy. Dokáže informovať operátorov a vývojárov, čo sa deje. Tieto informácie sa použijú na riadenie výkonnosti, bezporuchovosti ako aj škálovania spustených aplikácií a samotnej platformy
- Zabudovaná bezpečnosť chráni pred bezpečnostnými hrozbami aj vďaka automatickej aplikácii iných bezpečnostných kontrol na izolovanie aplikácií a dát
- Využitie riadenia prístupu na základe rolí (RBAC),
- Platforma by mala byť štruktúrovaného typu pretože poskytuje vstavané funkcie a integračné body pre spustenie aplikácií opakovateľným spôsobom. Pričom je postavená a nekompromisne dodržiava sadu vhodne definovaných zásad – princípov a postupov.
- PaaS platrofma by mala byť otvorená v troch dôležitých rovinách
    - pre výber IaaS vrstvy
    - z pohľadu množstva rôznych rámcov pre vývojárov, polyglot jazykov a aplikačných služieb
    - z pohľadu licencovania

IaaS

Navrhovaná architektúra musí vedieť poskytnúť služby virtuálneho datacentra cez zdieľanú multitenantnú platformu a taktiež poskytnúť dedikovaný privátny cloud, ktorý ponúka dedikovanú hardware platformu s flexibilitou vo viacerých vysoko dostupných dátových centrách pre všetky organizácie v rámci rezortu cez samo-obslužný portál, ktorý poskytuje užívateľom vysokú flexibilitu.

Kľúčové požiadavky na služby virtuálneho datacentra pre organizácie v rámci rezortu sú nasledovné:

- Multitenantný hardware (compute, storage and network)
- Garantované výpočtové zdroje
- Výpočtové zdroje (CPU a RAM) musia byť poskytnuté ako virtuálny „resource pool“ bez priameho prepojenia na fyzický server s možnosťou škálovania RAM aj CPU

- Diskový priestor (tiers) musí byť poskytovaný tiež cez „resource pool‘s“
- Musí byť možnosť zdieľať „resource pool“ cez viac serverov, alebo cez špecifický/konkrétny hardware
- Možnosť presúvať „resource pool“ v rámci celej platformy z dôvodu údržby alebo migrácie
- Užívateľ si môže sám vytvárať virtuálne servre, siete (VLAN), firewalls, LB, switching, routing, IP adresáciu a všetko čo má súvis s IaaS
- Užívateľ musí mať možnosť prístupu k verejnému katalógu s dostupnými images
- Užívateľ musí mať možnosť vytvoriť si vlastný katalóg s templates a images
- Užívateľ musí mať možnosť cez samoobslužný portál meniť konfiguráciu firewallu, LB, vytvárať, upravovať a mazať siete
- Možnosť spravovať kapacity v rámci celej platformy (zdieľané aj dedikované)
- Možnosť vyčísliť spotrebované HW zdroje
- Schopnosť ponúknuť licencovaný OS pre prípad, že užívateľ nechce použiť vlastný
- Samoobslužný portál pre užívateľov s GUI aj API s možnosťou definovať role (užívateľ/zákazník môže mať read-only užívateľov a ostatný užívatelia majú napr. obmedzený prístup k zmenám v celom virtuálnom datacentre)
- Samoobslužný portál musí byť dostupný cez linku (ideálne SSO)
- Všetky zmeny vykonané cez portál musia byť zaznamenané a dostupne administrátorom
- V rámci virtuálneho datacentra môže užívateľ vidieť a spravovať len svoje VM
- Podpora snapshot-based backup

Kľúčové požiadavky pre hostovaný dedikovaný privátny cloud sú nasledovné:

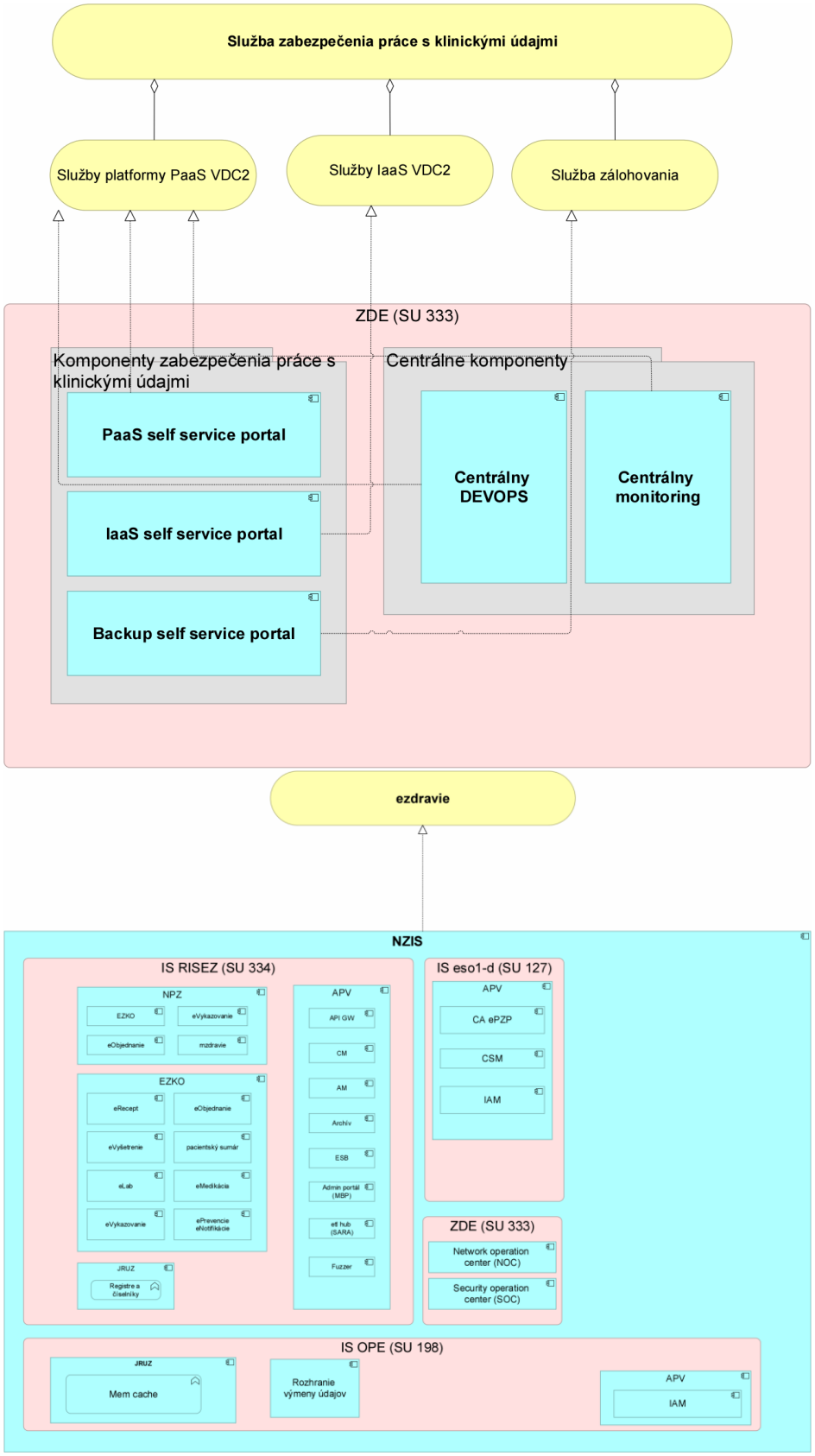
- Platí to isté ako pre virtuálne datacentrum s doplnením:
- Zdieľaný storage s možnosťou doplnenia dedikovaného storage hardware
- Snapshots, application-aware a file level backup

Pre umožnenie nasadenia cloud manažment nástrojov je v tejto štúdii uvažované s plne hyperkonvergovanou architektúrou s nutným využitím NSX a VSAN technológií.

Požiadavky na akýkoľvek návrh virtuálnej infraštruktúry sú aby bola zabezpečená škálovateľnosť cez desiatky fyzických serverov, ktoré vedia poskytnúť rádovo petabytes diskového priestoru s podporou komplexného virtuálneho networkingu. Pre úspešné nasadenie takejto infraštruktúry je nevyhnutná dokonalá správa, dodržiavanie pravidiel a odporúčaní a v neposlednom rade aj bezpečnosť. Toto je možné dodržať aj pomocou preddefinovaných stavebných blokov navrhovanej architektúry, ktoré je možné jednoducho škálovať podľa potreby od prvého dňa.

Dôležitým faktorom je aby bolo možné výpočtový výkon celej infraštruktúry flexibilne podľa potrieb rozdeľovať medzi organizácie rezortu, DevOps, atd. So zachovaním úplného oddelenia týchto zdrojov. Infraštruktúra pre zabezpečenie prevádzky a služieb pre organizácie (backend) bude oddelený od hardware-ových zdrojov, ktoré budú poskytované organizáciám v rámci rezortu.

Priestor pre sumárny obrázok: ArchiMate štandardný viewpoint – „Application Usage Viewpoint", „Application Co-operation Viewpoint"


Služba zabezpečenia práce s klinickými údajmi
Služby platformy PaaS VDC2
Služby IaaS VDC2
Služba zálohovania
ZDE (SU 333)
Komponenty zabezpečenia práce s klinickými údajmi
PaaS self service portal
IaaS self service portal
Backup self service portal
Centrálne komponenty
Centrálny DEVOPS
Centrálny monitoring
ezdravie
NZIS
IS RISEZ (SU 334)
NPZ
EZKO
eVykazovanie
eObjednanie
mzdravie
EZKO
eRecept
eObjednanie
eVyšetrenie
pacientský sumár
eLab
eMedikácia
eVykazovanie
ePrevencie eNotifikácie
JRUZ
Registre a číselníky
APV
API GW
CM
AM
Archív
ESB
Admin portál (MBP)
eII hub (SARA)
Fuzzer
IS eso1-d (SU 127)
APV
CA ePZP
CSM
IAM
ZDE (SU 333)
Network operation center (NOC)
Security operation center (SOC)
IS OPE (SU 198)
JRUZ
Mem cache
Rozhranie výmeny údajov
APV
IAM

Ďalšie informácie
(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)

Prílohy

Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.

Diagramy, modely, obrázky v plnom rozlíšení

Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

Technologická architektúra

Tabuľka 13 Technologická architektúra - budúci stav

Súhrnný popis

Celková architektúra riešenia pozostávajú z týchto základných blokov:

- virtuálne datacentrum 1 (vDC1) určené pre základné komponenty ESZ a JRUZ

- infraštruktúra pre virtuálne desktopy určená pre bezpečnú správu virtuálnych datacentier

- virtuálne datacentrum 2 (vDC2) určené pre nové rozvojové projekty rezortu zdravotníctva a ďalšie zapojené organizácie zdravotníctva

Virtuálne datacentrum 1

Prostredie určené pre základné komponenty ESZ a JRUZ (vDC1)

Architektúra vDC1 je založená na niekoľkých hlavných komponentoch:

- virtualizačná platforma a jej rozširujúce komponenty

- diskový subsystém

- zálohovací subsystém

Virtualizačná platforma

Virtualizačná platforma zabezpečuje bezvýdavkovú prevádzku virtuálnych strojov, ich migráciu počas behu virtuálneho stroja (výkon aj virtuálne disky), distribuované rozdelenie záťaže - automatická migrácia VM v prípade preťaženia fyzického servera alebo dátového úložiska, podporu optimalizácie fyzickej pamäte, rezervácie procesorového výkonu a pamäte, podporu pre logické združovanie zdrojov pre rôzne skupiny a virtuálny switch, ktorého konfigurácia je automatický distribuovaná na všetky fyzické servery pridané do tohto switcha.

Rozšírené funkcionality virtualizačnej platformy:

- komponent zabezpečujúci doplnenie funkcionality distribuovaného prepínania (switching) a smerovania (routing). Zároveň zabezpečuje firewalling na úrovní virtuálnej sieťovej karty virtuálneho stroja s podporou integrácie s Active Directory a bezpečnostných komponentov tretích strán. Ďalšími vlastnosťami sú:

- mikrosegementácia s ohľadom na kontext (napr. identifikácia aplikácii)

- monitoring a viditeľnosť prevádzky

- podpora plánovania pravidiel pre firewally

- univerzálny kolektor pre logy a nad nimi postavená analytika s implementovanou podporou pre znalosti pre danú virtualizačnú platformu

- nástroj pre monitoring výkonu a pokročilú analytiku nad týmito údajmi. Zároveň zabezpečuje správu a plánovanie kapacít, monitoring Operačných systémov a automatické rozloženie záťaže na základe historických údajov.

Diskový subsystém

Diskový subsystém pozostáva z dvoch diskových polí, každý umiestnený v jednom z fyzických datacentier (primárna a záložná lokalita). Tieto diskové polia sú navzájom prepojené, aby bola umožnená ich vzájomná synchronizácia (synchrónna alebo asynchrónna). Tieto diskové polia majú funkcionalitu kryptovania dát na nich uložených.

Zálohovací subsystém

Zálohovací subsystém pozostáva z fyzického zariadenia a zo systémov určených pre

- správu a monitoring replikácii a zálohovania

- plánovanie a realizáciu plánov obnovy

Fyzické zariadenia slúži na ukladanie záloh, podporuje kryptovanie týchto dát a zároveň umožňuje pristupovať k údajom pomocou protokol NAS, NFS, CIFS (SMB), iSCSI and FC virtual tape libraries (VTL).

Sieťová infraštruktúra

Architektúra

Sieťová infraštruktúra je rozdelená do nasledujúcich subsystémov a blokov. Každý z nich má špecifické vlastnosti a je dedikovaný na plnenie konkrétnych úloh.

Riešenie dátového centra bude pozostávať z nasledovných častí:

- Produkčná sieťová infraštruktúra dátového centra
    - Perimeter:
        - Internet peering
        - Prístupová vrstva
- Internal
    - Agregačná vrstva
    - Prístupová vrstva

- SAN infraštruktúra
- Manažmentová sieť DC prostredia

Produkčná sieťová infraštruktúra DC prostredia:

- Predstavuje infraštruktúru zabezpečujúcu komunikáciu jednotlivých produkčných komponentov IS. Interná zóna bude využívať technológie overlay siete.

SAN infraštruktúra:

- SAN infraštruktúra je zdieľané sieťové prostredie spolu s produkčnou sieťovou infraštruktúrou pre pripojenie a zabezpečenie komunikácie dátových úložísk a zálohovacích komponentov so serverovými komponentmi umiestnenými v produkčnej časti prostredia IS.

Manažmentová sieť DC prostredia:

- Manažmentová sieť je dedikované sieťové prostredie zabezpečujúce komunikáciu prvkov realizujúcich správu zariadení umiestnených vo všetkých ostatných časti prostredia IS. Správa zariadení je realizovaná výlučne z tejto siete. Táto časť zabezpečuje aj monitoring a správu sieťovej infraštruktúry.

V návrhu riešenia sa požaduje vysoká dostupnosť s využitím primárnej a záložnej lokality.

Požaduje sa nasledovná sieťová konektivita:

- Internet – samostatné dual homované pripojenie pre každú lokalitu(primárnu a záložnú)
- Prepojenie DC – redudantne na úrovni Ethernet/IP a Fibre channel

Infraštruktúra pre virtuálne desktopy (VDI)

VDI poskytuje podporu pre prístup k virtuálnym desktopom s OS Windows resp. Linux určených pre bezpečnú správu virtuálnych datacentier. Zároveň umožňuje podporu single sign-on pre aplikácie a desktopy, podporu dynamickej správy aplikácii pre jednotlivých užívateľov v reálnom čase, podporu správy používateľov, ich profilov a na nich aplikovaných politík.

Ako diskových subsystém pre túto infraštruktúre je použitá technológia softvérovo definovaného diskového systému, ktorá ako úložisko používa fyzické disky jednotlivých serverov umiestnených v klastri pre túto infraštruktúru. Tento klaster je distribuovaný medzi obe fyzické dátové centra z dôvodu vysokej dostupnosti.

Virtuálne datacentrum 2

Prostredie pre nové rozvojové projekty rezortu zdravotníctva a ďalšie zapojené organizácie zdravotníctva (vDC2)

PaaS

Paltforma PaaS spolu s jej platformovými službami musí umožniť používateľom nasadzovať a prevádzkovať CNA aplikácie, ktoré sú naprogramované v najtradičnejších programovacích jazykoch a programovacích rámcoch (frameworks), ale aj nových jazykoch a rámcoch, ktoré vznikli a sú optimalizované pre prostredie cloudu. Ide najmä o nasledovné programovacie rámce:

- **Java**
- **.NET**
- **Node.js**
- **GO**
- **PHP**
- **Python**
- **Ruby**

PaaS platforma poskytne v rámci svojej funkcionality tieto programovacie rámce aj potrebné komponenty pre beh aplikácii napísaných v daných programovacích rámcoch. Typicky ide napr. v prípade Javy, JRE, Tomcat java kontajner server agentov, jdbc ovládače a podobne (Pre účely štúdie sme vychádzali z platformy Cloud foundry kde je toto realizované pomocou tzv. buildpackov, ktoré sú pre vyššie uvedené rámce predpripravené, ale je požadované aby bolo možné vytvárať aj ďalšie vlastné buildpacky). Rovnako by platforma mala umožňovať nasadenie:

- **Aplikácie so statický súborovým kódom** - Aplikácia alebo obsah, ktorý nevyžaduje žiadny back-end kód, iný ako webový server. Príkladmi statických súborov sú:
    - front-endové JavaScript aplikácie
    - statický obsah HTML
    - formuláre typu HTML / JavaScript.
    - **Binárne balíky -** pre spustenie ľubovoľných binárnych webových serverov.

IaaS

Stavebný blok

Návrh stavebného bloku optimalizovaného pre jeden rack, obsahuje:

1. Rack s minimálnym výkonom 6kW
2. 2x leaf switch, kde každý switch ma 48 portov 10/25 Gbps a 6 portov 40Gbps
3. 1x OOB management switch pre prístup k servisným procesorom cez štandardný IPMI protokol
4. 5x 2U chassis, kde každé Chassis obsahuje 4 servere s parametrami:

    -
    - Memory: 384 GB
    - CPU: 2x Intel Xeon Gold 6150, 36 Cores
    - Network: 2x 25Gbps SFP, 2x 10Gbps RJ45, 1x 1Gbps IPMI Servisný procesor
    - Storage: 4x 3.84 TB NVMe SSD, 2x 1.6 TB NVMe SSD Cache

Jeden stavebný blok (rack) obsahuje teda nasledovnú výpočtovú kapacitu:

- 7,5 TB RAM
- 720 fyzických jadier (vcore)
- 305 TB NVMe SSD RAW Capacity (storage)

Licencovanie

Pre účely štúdie sme vychádzali z licenčných modelov

- VMWare - VCPP program pre Cloud Providerov. Všetky VMware Licencie sú v tomto modeli zahrnuté a platí sa minimálny poplatok 300,- € mesačne plus spotrebovaná RAM
- Microsoft licencovanie (ak bude potrebné zabezpečiť tieto licencie) navrhujem riešiť pomocou SPLA programu pre service providerov. Obdobne ako pri VMware poskytovateľ bude platiť na mesačnej báze iba za použite licencie. Ceny za mesačný prenájom Microsoft licencií sú určite priaznivejšie ako ich nákup ihneď. Naviac je možné, že v niektorom mesiaci bude platba nižšia, lebo sa nevyužije toľko licencií ako v predchádzajúci.

Networking

Architektúru networkingu navrhujem v designe Leaf-Spine, kde fyzické switche využijeme len ako rýchle prepoje bez zásadnejšej logiky. Kompletný networking a jeho logika bude riešená pomocou VMware NSX technológie, ktorá je postavená na VXLAN štandarde. Taktiež bude pomocou NSX zabezpečené load balancre, firewalls, dynamicky/statický routing ako softwarové apliancie. Tieto si budú organizácie konfigurovať vo vlastnej réžii. Taktiež si budú môcť v rámci svojich virtuálnych datacentier tieto sieťové zariadenia konfigurovať a vytvárať L2 siete. Na fyzických switchoch musí byť taktiež možné ukončiť VXLAN kompatibilnú s VMware NSX.

Takto koncipovaný networking bude základom pre IaaS, ale zároveň je s ním počítané aj na úrovni PaaS technológii, ktoré dynamicky konfigurujú networking podľa nasadzovaného workloadu.

Pripojenia jednotlivých serverov budú využívané na management traffic, storage traffic, traffic organizácií a taktiež traffic smerujúci z a do internetu (napr. IPSec,...) Navrhujem v plnej miere využiť výhody hyperkonvergovanej infraštruktúry. Pripojenie organizácii bude zabezpečené cez Internet, alebo govnet sieť spolu s IPSec tunelom LAN-to-LAN. Pre Väčšie organizácie bude možné pripojiť dedikovné linky priamo na ich virtuálne datacentrum.

Pre zabezpečenie najlepšej dostupnosti sa pre účely štúdie uvažuje pripojenie do internetu cez minimálne 2 internet operátorov. Taktiež ideálne je vlastne AS (autonomous system) - vlastný verejný IP adresný priestor v rámci internetu.

Storage

Riešenie úložiska navrhujeme z veľkej miery s využitím VMware vSAN technológie, ktorá automaticky zabezpečuje synchronizáciu dát naprieč clustrom a je možné definovať storage politiku per objekt (napr. HDD disk vo virtuálnom serveri). Technológia v maximálnej miere zjednodušuje prevádzku, poskytuje maximálnu mieru škálovateľnosti a využíva navrhnuté integrované NVMe disky v serveroch (s mimoriadne vysokými IOPS). Čiže pri rozšírení výpočtového výkonu sa automaticky rozširuje aj disková kapacita. Taktiež uvažujeme s tým, že bude možné pripojiť existujúce alebo legacy samostatné diskové polia, poprípade NAS pre zálohy pomocou iSCSI, alebo NFS protokolov.

Zálohovanie

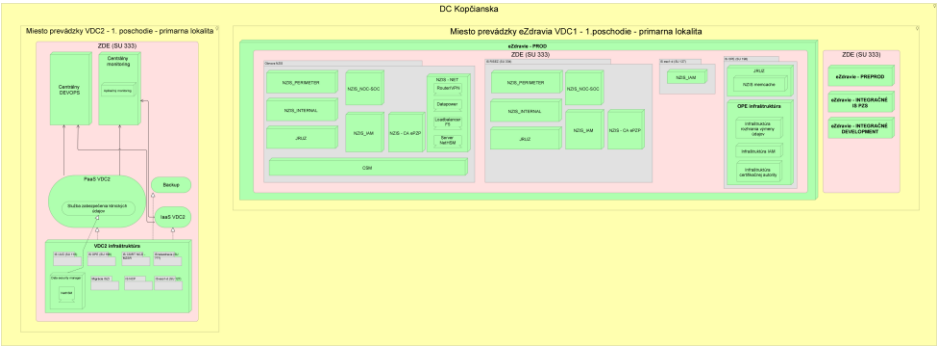
Pre riešenie zálohovania sú zohľadnené nasledujúce princípy:

- Riešenie musí podporovať multitenant režim (organizácie si musia vedieť sami konfigurovať politiku zálohovania a obnovy
- Riešenie musí podporovať zálohovanie na úrovni fyzických, virtuálnych serverov, kontajnerov a podporovať aplikačné zálohovanie

- Riešenie musí podporovať inštaláciu a beh v dvoch lokalitách pre zabezpečenie BCM a DRP

Pre účely štúdie vychádzame z technológie technológie Veeam, ktorá umožňuje aj Application aware zálohovanie (napr. vieme obnoviť len konkrétny email, alebo len časť databázy). Veeam umožňuje okrem politiky pre zálohovanie aj archivovať. Okrem zálohovania virtuálnych serverov je možné zálohovať aj fyzické servre na báze OS Linux, Windows a Mac. Taktiež je možné implementovať a prepojiť Veeam s VMware vCloud Directorom, kde si organizácie budú môcť sami konfigurovať backup politiku per VM a taktiež urobiť restore VM v prípade potreby.

Priestor pre sumárny obrázok: ArchiMate štandardný viewpoint – „Infrastructure Usage Viewpoint", „Infrastructure Viewpoint"



Ďalšie informácie
(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)

Prílohy

Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.

Diagramy, modely, obrázky v plnom rozlíšení

Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

Implementácia a migrácia

Tabuľka 14 Implementácia a migrácia

Súhrnný popis

Obsahovo je projekt rozdelený do 7 etáp v celkom časovom rozmedzí cca. 2 rokov. Projekt dodáva 3 samostatné delivery a to postavenie primárnej lokality PL pre VDC1 a VDC2 a zmigrovanie existujpúceho riešenia NZIS na novú infraštruktúru s vytvorením 4 prostredí (DEV, INTG, PREPROD a PROD)ako súčasti migrácie . Každá z etáp, tak ako je uvedené na nasledujúcom obrázku je samostatnou iteráciou, od zberu a spresňovania biznis požiadaviek cez realizáciu až po nasadenie a otestovanie . Týmto postupom sa snažíme eliminovať riziká vyplývajúce z toho, že sa jedná o vecne rozsiahly projekt a nie je možné dosť dobre vypracovať iba jednu obrovskú špecifikáciu bez toho aby sa na niečo nezabudlo a neskôr bol problém zabudnuté veci dopracovať.

Z pohľadu migrácie NZIS bude plán pre realizáciu vychádzať z nasledovného plán migrácie konzultovaného počas PTK:

1. Etapa návrhu riešenia – Etapa1 a 3
    1. Stanovenie a potvrdenie architektonických princípov pre VDC1 a VDC2
    2. Stanovenie a potvrdenie komplementárnych bezpečnostných princípov
    3. Návrh monitoringu bezpečnostných incidentov
    4. Návrh monitoring prevádzkových incidentov
    5. Návrh novej SDL v2
    6. Návrh architektúry VDC1
    7. Návrh architektúry VDC2
    8. Vytvorenie nové modelu hrozieb
    9. Návrh nutných zmien v komponentoch NZIS (na základe potvrdených architektonických princípov pre VDC1)
    10. Aktualizácia bezpečnostného projektu
    11. Vypracovanie nových prevádzkových postupov
    12. Vypracovanie nového release managementu
2. Etapa vybudovania VDC1 ako IaaS – Etapa 2
    1. Dodávka HW komponentov, systémového a databázového SW
    2. Nasadenie a konfigurácia prostredia VDC1 – primárne

    i. Network

        1. JRUZ
        2. Ident & Auth Edge
        3. Wan edge
        4. Internal
        5. Perimeter
        6. Internet edge

    ii. SAN

    iii. SQL

    iv. Vykonanie overenia technológie (Proof of Concept)

    1. Nasadenie a konfigurácia monitoringu bezpečnostných komponentov
    2. Nasadenie a konfigurácie monitoring prevádzkových komponentov
    3. Príprava DRP a BCM postupov a ich aplikácia v režime active-passive.

3. Etapa migrácie NZIS do VDC1 – etapa 4 až 7

1. Realizácia nutných zmien v komponentoch NZIS
    1. Migrácia na najnovšie platformové produkty
    2. Migrácia GUI na novú technológiu
    3. Migrácia NPZ na nový CMS systém
    4. Náhrad už nepodporovaných produktov a funkčností
2. Nasadenie, konfigurácia resp. migracia databáz serverov podľa sieľových zón v poradí:
    1. JRUZ
    2. ESB
    3. Autorizácia
    4. IAM
    5. Archív
    6. Fuzzer
    7. CM
    8. Admin portál
    9. ePreskripcia a eMedikácia
    10. eVysetrenie
    11. Pacientsky sumár
    12. eLab
    13. eObjednávanie
    14. eNotifkácie
    15. EZKO
    16. NPZ
    17. SARA
3. Sieťové presmerovanie zóny
4. Etapa vybudovania VDC2 ako PaaS – etapa 1 až 4
    1. Dodávka HW komponentov, systémového a databázového SW
    2. Nasadenie a konfigurácia prostredia VDC2

Implementačný plán bude vychádzať z architektonických princípov, ktoré budú zohľadnené v nasledovnom rozsahu pre VDC1, pričom počas úvodných etáp s cieľom overiť ich počas PoC môžu byť ešte spresnené. Výstup je konzultáciou počas PTK a uvádza sa v tvare ako bol predložený:

Jeden repozitár zdrojového kódu pre jednu „aplikáciu

Áno naplniteľný: Pokiaľ NCZI zabezpečí ako predpoklad centrálny repozitár zdrojového kódu, nastaví procesy a role a zabezpečí aktívnu prevádzkovú podporu, je tento bod možné splniť.

Alternatívne sa to dá vnímať ako splnené s tým že to bude zabezpečené v rámci SLA – táto alternatíva bola zamietnutá počas PTK.

Explicitná deklarácia a izolácia závislostí aplikácie.

Áno naplniteľný: Štandardne máme závislosť na .net framework. Pokiaľ sa toto vie považovať za akceptovateľne, tak ide o niektoré drobné úpravy (odstránenie závislosti od WIF – windows identity foundation), odkazovanie na pkcs11 knižnice hsm a pod + kompletne otestovanie nasadenia

1. **Konfigurácia (aplikácie) súčasťou prostredia, nie aplikácie.**

Áno naplniteľné: toto by vyžadovalo rework (+ vydanie všetkých modulov a ich poriadne testovanie) ako sú aplikácie konfigurované – potenciálne prehodnotenie aké bezpečnostné dopady môže mať iné nastavovanie konfigurácií (+ ochrana zmien konfigurácie)

2. Nezávislosť aplikácie od konkrétneho poskytovateľa podpornej služby back-endu.

Kritické: toto môže byť dosť náročné.

3. Jasné oddeľovanie jednotlivých štádií transformácie zdrojového kódu na bežiacu aplikáciu.

Áno naplniteľný: ako prvý princíp

4. Spustená aplikácia beží ako jeden alebo viac bezstavových procesov.

Áno naplniteľný: Malo by byť ok pre služby, pre weby je otázne či aplikovať princíp

5. Aplikácia je sama zodpovedná za publikáciu svojich komunikačných koncových bodov (portov).

Áno naplniteľný: pokiaľ sa zruší závislosti na IIS (obtiažne)- narocnost prepisania na SVC, resp. zruší závist na IIS. zavislosti na sharepoint (kritické)

6. Jednoduché škálovanie výkonu pomocou spúšťania a zastavovania (paralelných) bezstavových procesov.

Áno naplniteľný: spĺňa , sú potrebné zmeny na esb a load balancingu

Pre IIS platí ale pre služby SVC to neplatí.

7. Okamžité reakcie procesov na požiadavky spustenia a zastavenia

Áno naplniteľný: Vyžaduje splnenie bodu 7 + je možné optimalizovať čas spustenia

8. Minimalizovať rozdiely medzi prostrediami (najmä vývojovým a produkčným).

Áno naplniteľný: Toto by sa migráciou do cloudu vyriešilo, odlišne sady certifikátov

9. Aplikácia nikdy neriadi (a nespolieha sa na proprietárny) spôsob spracovania logov.

Áno naplniteľný: Toto si vyžaduje úpravy na úrovni adaptérov, ktoré realizujú zápis logov

10. Admin/manažment úlohy sú vyvíjané a vykonávané ako jednorazové procesy

Áno naplniteľný

11. Maximalizáciu robustnosti a minimalizáciu výpadkov aplikácie,

Áno naplniteľný: modré/ zelené nasadzovanie vyžaduje špecifický prístup a obmedzenia pri úpravách DB štruktúr

12. Vývojové/integračné/produkčné prostredia musia byť optimalizované na minimálny čas spustenia

Áno naplniteľný: Pridanie aplikačných nodov vidíme ako jednoduché

Kritické: Škálovanie DB pridávaním nodov ako problematické limitne nemožné

Kritické: Kontajnerizáciu ako realizovateľnú ale s veľkou prácnosťou s nutnosťou prepísať časti aplikácií

Pre VDC2 sa predpokladá naplnenie všetkých princípov:

Vychádzajúc zo ŠU projekt VDC2 počíta s využitím zdieľanej infraštruktúry vytvorenej z komoditného hardvéru, čo je aj jedným z prvých princípov uvedenej referenčnej architektúry ISVS. Ako už bolo spomenuté vyššie platforma PaaS a jej služby pomôžu vyskladať aplikácie vo VDC2 z jednotlivých vrstiev tak, aby sa využívali štandardné technologické komponenty, ktoré budú poskytované jednotlivým aplikáciám v rámci cloudovej platformy formou služieb s referenciou, čo je práve jedným z ďalších princípov ISVS v cloude, ale aj všeobecne známym princípom tzv. backingslužieb známym z manifestu 12factor.net prijatým vývojármi cloudových aplikácií.

Projekty vytvárané vo VDC2 umožnia vytvoriť podporné sub-doménové všeobecné a špecializované riešenia, ktoré budú zdielateľné medzi jednotlivými aplikáciami nasadenými nad budúcou PaaS platformu a umožnia ďalej zlepšiť nie len technické riešenia ale aj ekonomické hľadisko realizovaného

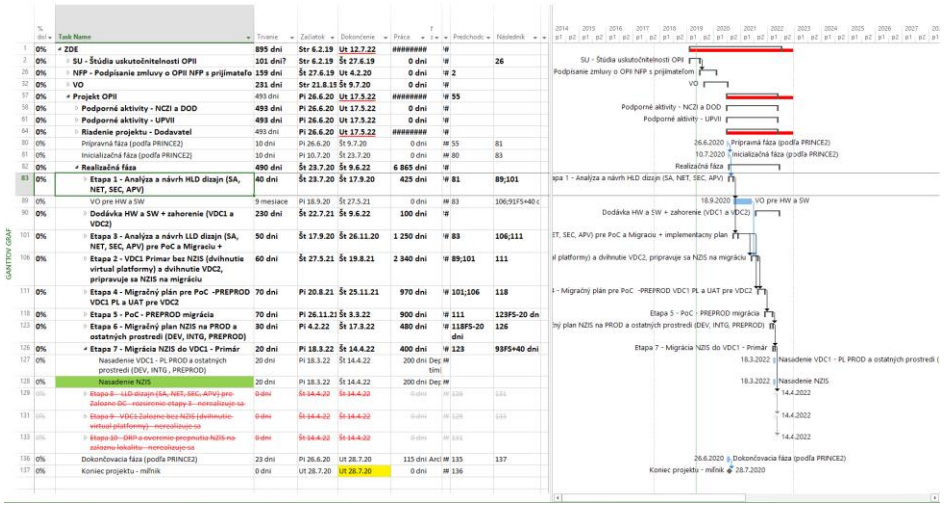
Princípy sú všeobecne platné pre tvorbu cloudových aplikácií nezávisle od programovacieho jazyka. Projekt eZdravia bude v prostredí VDC2 požadovať vytváranie aplikácií cloudového resp. cloud natívneho typu a teda musí NCZI od svojich dodávateľov vyžadovať aj princípy podľa manifestu https://12factor.net/ resp. princípy, ktoré vhodne preberá rozširuje aj referenčná architektúra ISVS v cloude.

Okrem uvedených princípov sa zvažuje využiť zavedenie princípov telemetrie, teda zberu prevádzkových informácií o nasadených aplikáciách v jednotlivých doménach o ich výkonnosti. Zavedenie správnej telemetrie umožní následne ľahšie auditovanie a monitorovanie nasadených cloudových aplikácií v prostredí VDC2.

Ďalším dôležitým princípom je bezpečnosť. Pôvodný manifest nepreberá bezpečnosť, avšak každá aplikácia v cloudovom prostredí vyžaduje zapuzdrenie bezpečnosti vrátane autentizácie a autorizácie. V ideálnom prípade bude potrebné na cloud natívne aplikácie aplikovať zabezpečenie pomocou definície rolí tzv. RBAC (role-based access control). Pričom pri každej

požiadavke na aplikáciu musí byť jasné kto požiadavku vykonal a k akej role takáto požiadavka patrí

Jednotlivé výstupy projektu a ich zaradenie do etáp je uvedené v nasledujúcej tabuľke. Spoločné aktivity predstavuje aktivity, ktoré sa týkajú všetkých výstupov a ich hlavným účelom je zabezpečiť to aby bol projekt realizovaný načas v správnej kvalite a s adekvátnou úrovňou bezpečnosti.



	% dok	Task Name	Trvanie	Začiatok	Dokončenie	Práca	Predchodc	Následník
1	0%	ZDE	895 dni	Str 6.2.19	Ut 12.7.22	########	#	
2	0%	SU - Štúdia uskutočnitelnosti OPII	101 dni?	Str 6.2.19	Št 27.6.19	0 dni	#	26
26	0%	NFP - Podpisanie zmluvy o OPII NFP s prijímateľo	159 dni	Št 27.6.19	Ut 4.2.20	0 dni	# 2	
32	0%	VO	231 dni	Str 21.8.19	Št 9.7.20	0 dni	#	
57	0%	Projekt OPII	493 dni	Pi 26.6.20	Ut 17.5.22	########	# 55	
58	0%	Podporné aktivity - NCZI a DOD	493 dni	Pi 26.6.20	Ut 17.5.22	0 dni	#	
61	0%	Podporné aktivity - UPVII	493 dni	Pi 26.6.20	Ut 17.5.22	0 dni	#	
64	0%	Riadenie projektu - Dodavatel	493 dni	Pi 26.6.20	Ut 17.5.22	########	#	
80	0%	Pripravná fáza (podľa PRINCE2)	10 dni	Pi 26.6.20	Št 9.7.20	0 dni	# 55	81
81	0%	Inicializačná fáza (podľa PRINCE2)	10 dni	Pi 10.7.20	Št 23.7.20	0 dni	# 80	83
82	0%	Realizačná fáza	490 dni	Št 23.7.20	Št 9.6.22	6 865 dni	#	
83	0%	Etapa 1 - Analýza a návrh HLD dizajn (SA, NET, SEC, APV)	40 dni	Št 23.7.20	Št 17.9.20	425 dni	# 81	89;101
89	0%	VO pre HW a SW	9 mesiace	Pi 18.9.20	Št 27.5.21	0 dni	# 83	106;91FS+40 d
90	0%	Dodávka HW a SW + zahorenie (VDC1 a VDC2)	230 dni	Št 22.7.21	Št 9.6.22	100 dni	#	
101	0%	Etapa 3 - Analýza a návrh LLD dizajn (SA, NET, SEC, APV) pre PoC a Migraciu +	50 dni	Št 17.9.20	Št 26.11.20	1 250 dni	# 83	106;111
106	0%	Etapa 2 - VDC1 Primar bez NZIS (dvihnutie virtual platformy) a dvihnutie VDC2, pripravuje sa NZIS na migráciu	60 dni	Št 27.5.21	Št 19.8.21	2 340 dni	# 89;101	111
111	0%	Etapa 4 - Migračný plán pre PoC -PREPROD VDC1 PL a UAT pre VDC2	70 dni	Pi 20.8.21	Št 25.11.21	970 dni	# 101;106	118
118	0%	Etapa 5 - PoC - PREPROD migrácia	70 dni	Pi 26.11.21	Št 3.3.22	900 dni	# 111	123FS-20 dn
123	0%	Etapa 6 - Migračný plan NZIS na PROD a ostatných prostredi (DEV, INTG, PREPROD)	30 dni	Pi 4.2.22	Št 17.3.22	480 dni	# 118FS-20 dni	126
126	0%	Etapa 7 - Migrácia NZIS do VDC1 - Primár	20 dni	Pi 18.3.22	Št 14.4.22	400 dni	# 123	93FS+40 dni
127	0%	Nasadenie VDC1 - PL PROD a ostatnych prostredi (DEV, INTG , PREPROD)	20 dni	Pi 18.3.22	Št 14.4.22	200 dni	Dep # tim	
128	0%	Nasadenie NZIS	20 dni	Pi 18.3.22	Št 14.4.22	200 dni	Dep #	
129	0%	~~Etapa 8 - LLD dizajn (SA, NET, SEC, APV) pre Zalozno DC - rozsirenie etapy 3 - nerealizuje sa~~	~~0 dni~~	~~Št 14.4.22~~	~~Št 14.4.22~~	~~0 dni~~	~~# 126~~	~~131~~
131	0%	~~Etapa 9 - VDC1 Zalozne bez NZIS (dvihnutie virtual platformy) - nerealizuje sa~~	~~0 dni~~	~~Št 14.4.22~~	~~Št 14.4.22~~	~~0 dni~~	~~# 129~~	~~133~~
133	0%	~~Etapa 10 - DRP a overenie prepnutia NZIS na zalozne lokality - nerealizuje sa~~	~~0 dni~~	~~Št 14.4.22~~	~~Št 14.4.22~~	~~0 dni~~	~~# 131~~	
136	0%	Dokončovacia fáza (podľa PRINCE2)	23 dni	Pi 26.6.20	Ut 28.7.20	115 dni	Arc # 135	137
137	0%	Koniec projektu - mílnik	0 dni	Ut 28.7.20	Ut 28.7.20	0 dni	# 136	

Výstupy projektu	Etapa 1 - 4 179 dní	Etapa 5-7 105 dní	Nutný / Preferovaný výstup
Spoločné aktivity			
Riadenie implementácie projektu	■	■	Nutný
Informačná bezpečnosť riešenia	■	■	Nutný
Dokumentácia	■	■	Nutný
Q&A počas projektu	■	■	Nutný
Špecifické výstupy			
VDC1 PL	■	■	Nutný
VDC2 PL	■		Nutný
Migrácia NZIS	■	■	Nutný

R_x: Riziko správnosti vyčíslenia nákladov projektu

R_x: Projekt nespĺňa Štúdiou stanovený harmonogram, rozpočet, alebo kvalitu.

R_x: Objednávateľom nepresná a neprimeraná definícia požiadaviek Štúdie na spôsob riešenia projektu.

R_x: Prirodzený odpor k využívaniu nového systému v dôsledku chýbajúcich skúseností s ním, ako aj nesprávneho pochopenia práce s novými funkcionalitami.

R_x: Neefektívne využite nových možností, ktoré ZDE prostredníctvom podporných nástrojov poskytne prevádzkovateľovi.

R_x: Riziko nedosiahnutia plánovaných kvalitatívnych prínosov projektu

Prílohy	**Diagramy, modely, obrázky v plnom rozlíšení**
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	*Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*

Bezpečnostná architektúra

Tabuľka 15 Bezpečnostná architektúra - budúci stav

Súhrnný popis

Navrhované architektúra zohľadňuje bezpečnostné požiadavky:

- existujúceho IS ESZ, ktoré bude súčasťou riešania
- vyplývajúce z nových legislatívnych požiadaviek
- na umiestnenie ďalších IS do riešenia/cloudu
- na ochranu pred novými typmi útokov

Výsledkom bude implementácia technických komponentov informačnej bezpečnosti, ktoré sú prierezovo integrované do celého riešenia. Navrhnuté komponenty spolu s procesnými opatreniami a ľuďmi predstavujú vzájomne spolupracujúci systém, pre dosiahnutie vysokej úrovne zabezpečenia nielen dôvernosti ale aj integrity a dostupnosti..

Vlastnosti riešenia:

- Súlad so Zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov a Vyhlášku Úradu na ochranu osobných údajov Slovenskej republiky č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobný údajov - nakoľko pôjde o IS obsahujúce a spracúvajúce osobné údaje.
- Súlad so Zákonom č. 275/2006 Z.z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov a Výnosom Ministerstva financií Slovenskej republiky č. 55/2014 Z. z o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov.
- Súlad s požiadavkami Zákona č. 69/2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a prostredníctvom jeho vykonávacích predpisov Vyhlášky Národného bezpečnostného úradu č.164/2018 Z. z. , ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby), Vyhlášky Národného bezpečnostného úradu č.165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov a Vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.
- Súlad s medzinárodnými normami a štandardmi, najmä STN EN ISO 27799:2017.
- Súlad s aktuálnymi odporučeniami CIS SANS inštitútu, DISA, a NIST.
- vypracované dokumenty bezpečnostnej politiky (úroveň policy/ practice / procedure) v súlade s bezpečnostnými štandardami pre verejnú správu, medzinárodnými normami a štandardmi, najmä STN ISO/IEC 27001:2014, STN ISO/IEC 27002:2014 a STN ISO/IEC 27005:2012 pre všetky bezpečnostne relevantné oblasti a technické bezpečnostné opatrenia vychádzajú zo schválených dokumentov bezpečnostnej politiky.
- Pokrýva nasledovné bezpečnostné riziká:
    - Únik citlivých informácií
    - Získanie neoprávneného prístupu, vrátané samotných administrátorov
    - Zmena citlivých informácií
    - Zmena programového vybavenia
    - Zmena spôsobu fungovania programu
    - Popretie vykonania akcie

    - Nedostatočné informácie pre preukázanie aktivity používateľa
    - A ďalšie
- Bezpečnostné mechanizmy sú návrhom členené do oblastí:
    - Dôvernosť a integrita
    - Sieťová bezpečnosť
    - Aplikačná bezpečnosť
    - Vynútenie bezpečnostnej stability prostredia
    - Antimalware ochrana
    - Monitorovanie bezpečnosti a reakcia na incidenty
    - Ochrana pred únikom informácií
- Prevádzkovanie Security Operation Centra - centrálny bod, ktorý:
    - monitoruje a vyhodnocuje bezpečnostnú situáciu pomocou nasledujúcich technológií:
        - SIEM technológie
        - Detegovanie anomálií
        - Zber plnej sieťovej prevádzky (*full packet capture*)
        - Monitorovanie interaktívnych činností administrátorov

- Aktívne chráni, tj, spravuje ochranné mechanizmy

množinou prvkov centrálnej správy bezpečnostných komponentov, ktoré sú integrované a koordinované s IRT

- Bezpečnostne relevantné rozhodnutia v oblasti architektúry, stanovení sily bezpečnostných mechanizmov a výbere konkrétnych technických riešení budú na základe realizovanej a schválenej analýzy rizík.
- Riešenie bude poskytovať možnosť segregácie rolí (segregation of duties) – administratívne oddelené budú od seba role, ktorých spojenie by predstavovalo bezpečnostné riziko na základe schválenej analýzy rizík a bezpečnostnej politiky.
- Ochrana do hĺbky kombináciou prevenčných, detekčných a eliminačných opatrení. Dizajn bude dôsledne implementovať realizáciu ochrany do hĺbky, čím sa minimalizuje dopad prípadného zlyhania niektorého z opatrení.
- Riešenie bude škálovateľné
- Riešenie bude natívne vysoko dostupné s podporou loadbalancingu
- Riešenie bude podporovať dynamické prideľovanie zdrojov pre schválené projekty s prvkami automatizácie
- Riešenie bude poskytovať prvky automatizácie pri aplikácii rôznych bezpečnostných politík formou šablón, viazanie politiky je možné aj priamo na aktívum (asset),
- Riešenie bude obsahovať komponenty pre zálohovanie a archiváciu dát.
- Riešenie bude umožňovať definovanie afinity pravidiel
- Riešenie bude obsahovať prevádzkový monitoring komponentov a častí riešenia

- Riešenie bude odolné voči katastrofám lokálneho charakteru. Plánovanie kontinuity činností bude súčasťou návrhu tak, aby v súlade s definovanou stratégiou obnovy boli jasne deklarované a následne zabezpečené požadované časy obnovy a dostupnosti riešenia
- Riešenie bude umožňovať fyzické a logické oddelenie niektorých zón a prostredí (napr. perimeter od internal) na všetkých úrovniach (sieťovej aj výpočtovej)
- Riešenie bude umožňovať fyzické a logické dedikovanie výpočtových kapacít pre vybrané druhy komponentov s možnosťou ich škálovateľnosti
- Riešenie bude umožňovať fyzické a logické dedikovanie diskových kapacít pre vybrané zóny s možnosťou ich škálovateľnosti
- Riešenie bude umožňovať integráciu komponentov typu aplliance (komponent pozostávajúci z kombinácie HW a SW priamo definovaného/dodávaného vendorom) s možnosťou ich škálovateľnosti
- Riešenie bude obsahovať komponenty na hw ochranu kryptografických kľúčov
- Prístup do riešenia bude povinne riadený až po úroveň jednotlivých komponentov, len na základe rolí.
    - Oddelenie správy:
        - Serverová infraštruktúra vs. disková infraštruktúra vs. sieťové prvky vs. bezpečnostné prvky
        - Sieťové a bezpečnostné komponenty rôznych typov/vrstiev/zón
        - Servery rôznych typov/vrstiev/zón
        - Diskový priestor rôznych typov/zón

- Fyzické priestory uloženia osobných údajov osobitnej kategórie budú v zabezpečenej zóne, pričom vstup používateľa do zóny s osobitnou kategóriou osobných údajov z iných zón bude vyžadovať osobitnú autentizáciu využitím tokenu alebo biometricky.
- Riešenie bude obsahovať bezpečnostné mechanizmy, ktoré:
    -
        - budú garantovať dôvernosť, dostupnosť a integritu osobných údajov.
        - umožnia aby aktuálny stav bezpečnosti bol multiúrovňovo (úroveň sieťovej a bezpečnostnej infraštruktúry, OS, databáz a aplikácií) on-line monitorovaný a vyhodnocovaný.
        - umožnia aby identifikované podozrivé aktivity a klasifikované bezpečnostné incidenty boli pri prekročení definovaného prahu závažnosti eskalované v súlade s definovanými eskalačnými procedúrami.
        - zabezpečia, aby databázy a dátové úložiská obsahujúce osobné údaje osobitnej kategórie boli chránené tak, aby aj pri využití, zneužití či kompromitácii prístupových práv oprávnených osôb na úrovni správcov bolo minimalizované riziko masovému úniku osobných údajov.
        - zabezpečia, aby pri prenose osobných údajov na úrovni point-to-point nedošlo k narušeniu dôvernosti a integrity osobných údajov.

- riešenie bude pozostávať z minimálne dvoch virtuálnych datacentier, v ktorých budú umiestnené aktuálne informačné systémy rezortu aj prípadné plánované projekty
- riešenie umožní geografickú vysokú dostupnosť pre každé virtuálne datacentrum (VDC)
- každé virtuálne datacentrum bude pozostávať z minimálne 3 klastrov – správa, produkčné virtuálne stroje a virtuálne stroje pre databázy
- každé virtuálne datacentrum bude obsahovať nasledujúce skupiny zdrojov, ktorých ich použitie v jednotlivých virtuálnych datacentrách závisí od potrieb informačných systémov v nich umiestnených:
  - hypervízory
  - dedikované fyzické servery
  - fyzické špecializované zariadenia
- VDC1 bude určené pre produkčné, preprodukčné, integračné a vývojové služby NZIS (prípadne špecifické systémy)
- VDC2 bude určené pre ostatné informačné systémy
- každé virtuálne datacentrum bude mať možnosť využiť pre uchovávanie dát fyzické dátové úložisko alebo softvérovo definované dátové úložisko resp. kombináciu týchto dvoch možností
- dátové úložiská obsahujúce osobné údaje osobitnej kategórie musia byť na fyzických dátových úložiskách
- infraštruktúra pre správu VDC bude oddelená od produkcie s riadeným prístupom
- riešenie bude obsahovať VDI prostredie, ktorá bude slúžiť na bezpečnú správu riešenia a jeho jednotlivých časti
- pre správu VDC1 bude slúžiť len VDI prostredie
- prístup a práca vo VDI prostredí bude striktne obmedzené a monitorovaná

Priestor pre sumárny obrázok / graf / diagram.

Prílohy	**Diagramy, modely, obrázky v plnom rozlíšení**
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	*Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*

Prevádzka

Tabuľka 16 Prevádzka - budúci stav

Súhrnný popis

Prevádzku komunitného cloudu bude zabezpečovať NCZI pomocou existujúceho tímu, ktorý prevádzkuje súčasný NZIS na úrovni L1 a L2. L3 zabezpečí budúci dodávateľ v súlade so stanovenými SLA požiadavkami. Na NCZI sa ráta s posilnením o devops zdroje a o zdroje potrebné pre rozšírenú prevádzku projektov umiestnených v rámci VDC2. Návrh zabezpečenia prevádzky predstavuje dôležitú súčasť projektových aktivít ako aj aktivít súvisiacich s trvalou udržateľnosťou riešenia počas horizontu minimálne ďalších 5 rokov.

Aktivity zabezpečenia prevádzky počas projektu na NCZI a dodávateľom riešenia:

- Prebehne zaškolenie a príprava tímu NCZI na nové technológie a nové prevádzkové procesy v súlade s novým riešením
- Bude odovzdané riešenie pre VDC1 a VDC2 do prevádzky NCZI a nasadený NZIS prevádzkou NCZI v súlade s migračným plánom a tak overené jeho úspešná migrácia na nové prostredia, vráatane overenia úplnosti a kvality dodanej dokumentácie.
- Rozšíri sa prevádzka o devops procesy, vrátane zaškolenia prevádzky na centrálne riadený devops
- Aplikuje sa nový release manažment, monitoring , zálohovanie a ostatné procesy v súlade s dodaným novým riešením vrátane ich overenia v súlade s dodanou dokumentáciou
- Rozšíri sa prevádzka o nové centrálne repozitory pre centrálne riadenie zdrojového kódu a jeho releasov, ako prvý sa overí centrálne riadený relaeas manažment nad centrálnym repository migrovaný NZIS s JRUZ
- Budú rozšírené procesy a dokumentácia pre Helpdesk a CallCentrum NCZI a ich podpora pre nové riešenie dodávateľom
- NCZI Preberie do správy a prevádzky všetky 4 prostredia po odovzdaní dodávateľom
- Prevádzka NCZI bude vysoko súčinná pri migrácii NZIS a JRUZ s cieľom zabezpečiť správne konfiguračné informácie a informácie o skutočnom nasadení prostredí
- Prevádzka NCZI bude súčinná v súlade so stanoveným projektovým plánom odsúhlaseným pre každú etapu RV.

Aktivity zabezpečenia produkčnej prevádzky:

- Riešenie bude nastavené tak, aby z dôvodu práce s vysoko citlivými dátami nebude mať L3 aktívny prístup do riešenia.
- L3 bude môcť byť udelený monitorovaný a auditovateľný prístup v obmedzenej miere napr. len ako read only prístup pre identifikáciu chýb. Rozsah rolí a oprávnení bude predmetom analýzy riešenia
- Devops tím bude s dodávateľom riešiť iba chyby a problémy, ktoré nebude schopný vyriešiť devops tím.
- Bude zabezpečovať služby v súlade so stanovenými SLA parametrami

Priestor pre sumárny obrázok / graf / diagram, nepovinná informácia.

Z hľadiska prevádzky navrhnutých riešení je potrebné uviesť, že riešenie navrhnuté v tejto štúdii rešpektuje aktuálne možnosti NZIS, nad ktorým bude vybudované. V prípade potreby iných riešení (napr. iných licenčných modelov, iných natívnych platforiem, atď) môžu byť prípustné aj iné ako tu navrhnuté a odporúčané riešenia za splnenia nasledovných podmienok:

- bude preukázaná reálna biznis potreba iných riešení,
- riešenie bude certifikované pre použitie v komunitnom cloude,

Kritéria kvality:

- Používateľská dokumentácia
- Prevádzková a administrátorská dokumentácia
- Možnosti testovania a školení (testovacie a školiace prostredie pre používateľov služieb)

Riziko

R_17: Zabezpečenie dostupnosti informačných systémov (najmä v prípade rozsiahlych havárií - disaster) nezodpovedá legislatívnym požiadavkám

R_22: Organizačné zabezpečenie podpory nedokáže včas vybudovať štruktúru s dostatočnými skúsenosťami a kvalifikáciou

Prílohy	**Diagramy, modely, obrázky v plnom rozlíšení**
Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.	*Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.*

Ekonomická analýza

Tabuľka 17 Ekonomická analýza - budúci stav

Súhrnný popis

Čistá súčasná ekonomická hodnota (ENPV) = 40 070 968,- EUR bez DPH

Rok návratu investície (PBP) = 5.rok

BCR (pomer prínosov a nákladov) = 4,1

Prínosy projektu sú stanovené na základe nasledujúcich faktorov:

- ušetrený čas lekárov pri opakovanom zakladaní receptu (v priemere 0,05 hod. trvania opakovaného zadania, 0,03 EUR – náklady na tlač),
- ušetrený čas lekárov a ZPr pri opakovanom zakladaní lekárskej správy (Tlač a podpísanie 1 lekárskej správy lekárom - 0,05 hod. Založenie papierovej zdravotnej dokumentácie zdravotnou sestrou - 0,05 hod. Načítanie 1 lekárskej správy a vykonanie podpísania zdravotnej dokumentácie ePZP kartou a elektronickým popisom - 0,05 hod. Zaslanie zdravotnej dokumentácie do NZIS - 0,02 hod., 0,03 EUR – náklady na tlač),
- ušetrený čas lekárov pri opakovanom zakladaní výsledkov laboratórnych vyšetrení (Tlač a podpísanie 1 laboratórneho výsledku lekárom – 0,05 hod. , 0,03 EUR – náklady na tlač, Poštovné 0,83 EUR, Obálka 0,03 EUR),
- ktoré boli spôsobené nedostupnosťou systému z dôvodu poruchy infraštruktúry (rozdiel medzi 97% a 95% dostupnosťou prostredia).

Údaje využité pri stanovovaní prínosov:

- vychádzajú z prevádzkových štatistík NCZI pre systém ezdravie,
- vychádzajú z meraní projektu Online procesy ezdravia pre stanovenie dĺžky trvania jednotlivých úkonov.

Celkové kapitálové výdavky projektu = 48 109 246, - EUR s DPH

Náklady projektu, tak ako sú uvedené v prílohe SU_ZDE - CBA a TCO - preferovana.xlsx sú stanovené na základe:

- Pre VDC1 – stanovením infraštruktúrnych prvkov a ich cien, ktoré vychádzajú z prvkov využívaných pri prevádzke ezdravia resp. ich komplementárnych (modernejších) náhradách. Sizing bol stanovený na základe sizingu systému ezdravie
- Pre VDC2 - stanovením infraštruktúrnych prvkov a ich cien, ktoré vychádzajú z prvkov využívaných pri výstavbe riešení s obdobnou architektúrou a KPI. Sizing bol stanovený na základe kapacitných požiadaviek rozvojových projektov.
- Odhadov prácnosti na základe dekompozície na menšie projektové celky.

Údaje využité pri stanovovaní nákladov, boli konzultované počas prípravy štúdie v rámci prípravnej trhovej konzultácie.

Priestor pre sumárny obrázok / graf / diagram, nepovinná informácia.

Ďalšie informácie
(Max. 1600 znakov, pre detailný popis je potrebné využiť prílohy)

Prílohy

Zoznam príloh. Prílohy obsahujú informácie v štruktúrovanej forme.