SPRÁVA ŽELEZNIC

Váš dopis zn.
Ze dne 42311/2023-SŽ-GŘ-O8
Naše zn.
Listů/příloh 3/2

Vyřizuje Miriam Hemzová
Mobil
E-mail Hemzova@spravazeleznic.cz

Datum 20. června 2023

Pozvánka k předběžné tržní konzultaci ve věci přípravy zadávacích podmínek na veřejnou zakázku s názvem *„Gamifikace kybernetické bezpečnosti Správy železnic, státní organizace.“*

Vážená paní, vážený pane,

Správa železnic, státní organizace (dále jen „*Zadavatel*“) Vás touto cestou informuje o přípravě podkladů pro uskutečnění řízení na veřejnou zakázku **„Gamifikace kybernetické bezpečnosti Správy železnic, státní organizace“**. Před samotným vyhlášením této veřejné zakázky bude předcházet předběžná tržní konzultace (dále také „*PTK*“) dle § 33 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „*Zákon*“). Cílem PTK je získat relevantní informace pro správné nastavení předmětu plnění, jednotlivých podmínek, volby druhu zadávacího či výběrového řízení dle interní směrnice Zadavatele a způsobu hodnocení předložených nabídek. Zadavatel usiluje, aby nastavené zadávací podmínky co nejlépe odpovídaly jeho potřebám a současně naplňovaly zákonné požadavky, zejména zásadu přiměřenosti a další zásady upravené v § 6 Zákona.

K povinnostem Zadavatele patří:

- plnění požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „*ZKB*“),
- plnění požadavků vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (dále jen „*VKB*“), a to ve smyslu § 9 Bezpečnost lidských zdrojů odst. 1 písm. a),
- plnění požadavků nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 (dále jen GDPR),
- plnění požadavků zákona č. 110/2019 Sb. o zpracování osobních údajů,
- dbát na soulad s normou ISO/IEC 27001:2013 - Příloha A – A.7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací.

V rámci opatření k naplnění výše uvedeného má Zadavatel v záměru uskutečnit řízení na veřejnou zakázku „Gamifikace kybernetické bezpečnosti Správy železnic, s.o.“, na jejímž základě bude uzavřena smlouva na implementaci informačního systému gamifikace kybernetické bezpečnosti, která pomocí zábavné formy školení „škola hrou“ motivuje zaměstnance k lepším výkonům ve vzdělávání v oblasti kybernetické bezpečnosti.

Správa železnic, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČO: 709 94 234 DIČ: CZ 709 94 234
www.szdc.cz

Správa železniční telematiky
V Celnici 1028/10
110 00 Praha 1

V příloze č. 1 této pozvánky je uvedena specifikace předmětu plnění veřejné zakázky, cílů a předběžných požadavků na řešení.

PTK je podle Směrnice Evropského parlamentu a Rady 2014/24/EU ze dne 26. 2. 2014 o zadávání veřejných zakázek a o zrušení směrnice 2004/18/ES a podle § 33 Zákona možností zadavatele předtím, než vyhlásí veřejnou zakázku, přičemž zadavatel má možnost v rámci PTK komunikovat s dodavateli (případně dalšími relevantními osobami) s cílem připravit zadání veřejné zakázky a informovat hospodářské subjekty (resp. dodavatele) o svých plánech a požadavcích při zadávání veřejných zakázek – zadavatel přitom může v rámci PTK i zjišťovat možnosti dodavatelů a případně i jejich návrhy řešení. Zadavatel se při využití PTK nesmí dopustit jednání, které by narušilo hospodářskou soutěž, tedy došlo by k neoprávněnému zvýhodnění jednotlivých potencionálních dodavatelů a také k jednání porušující zásady stanovené v § 6 Zákona.

Forma předběžné tržní konzultace: písemná

V rámci PTK žádáme o zodpovězení dotazů Zadavatele uvedených v příloze č. 2 této pozvánky. Odpovědi, které obdrží Zadavatel, budou pečlivě analyzovány a vyhodnoceny. S ohledem na účel PTK Zadavatel přihlédne i k opožděným odpovědím, bude-li to možné a vhodné pro účel PTK. Zadavatel však žádá účastníky, aby stanovené termíny dodrželi. Dojde-li Zadavatel k závěru, že některá témata zůstávají nadále nejasná, sporná či vyvstane potřeba objasnění dalších doplňujících dotazů, přistoupí Zadavatel ke konání dalšího kola PTK, které může být uskutečněno opět písemnou formou, případně si Zadavatel vyhrazuje možnost požádat zástupce dodavatelů o realizaci prezenčního jednání. Tento postup bude Zadavatelem opakován, dokud nebudou obdrženy veškeré informace potřebné ke správnému nastavení parametrů veřejné zakázky s názvem „Gamifikace kybernetické bezpečnosti Správy železnic, státní organizace". Zadavatel o dalším průběhu PTK osloví vždy minimálně ty dodavatele, kteří projevili zájem o PTK v předcházejícím kole.

V případě Vašeho zájmu o účast na této PTK zašlete své odpovědi na otázky uvedené v příloze č. 2 této pozvánky na emailovou adresu: **cnitptk@spravazeleznic.cz**.

Svoji odpověď prosím doručte nejpozději do 02. 07. 2023.

Dodavatel by ve své odpovědi měl uvést minimálně:

- název dodavatele a sídlo dodavatele;
- IČO dodavatele;
- jméno a funkce kontaktních osob, včetně kontaktních údajů (minimálně e-mail);
- odpovědi na přiložené otázky.

Pro bližší informace ohledně PTK se lze obrátit na tuto kontaktní osobu:

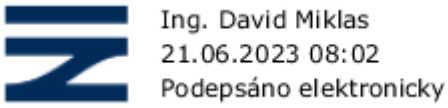
email: **cnitptk@spravazeleznic.cz**

Vzhledem k tomu, že PTK nesmí vést k porušení základních zásad dle § 6 Zákona a narušit hospodářskou soutěž, průběh i výsledek PTK bude zaznamenán ve zprávě vytvořené Zadavatelem. Informace z PTK užité v zadávacích podmínkách veřejné zakázky budou uvedeny v souladu s § 36 odst. 4 Zákona, a to včetně osob, které se na PTK podílely. Zadavatel současně uvede v zadávacích podmínkách i všechny

podstatné informace, které byly obsahem PTK a ovlivnily nastavení zadávacích podmínek.

Děkuji za spolupráci.

S pozdravem



Ing. David Miklas
ředitel Správy železniční telematiky

Přílohy:
Příloha 1 – Popis předmětu PTK
Příloha 2 – Otázky pro PTK

Předběžná tržní konzultace ke Gamifikace kybernetické bezpečnosti – příloha č. 1

Specifikace předmětu plnění

Zadavatel plánuje veřejnou zakázku s názvem „Gamifikace kybernetické bezpečnosti Správy železnic, s.o.". Cílem plnění veřejné zakázky je implementace informačního systému gamifikace kybernetické bezpečnosti, který pomocí zábavné formy školení „škola hrou" motivuje zaměstnance k lepším výkonům ve vzdělávání v oblasti kybernetické bezpečnosti.

Záměr Zadavatele v oblasti

Hlavním záměrem je nahrazení klasického statického e-learningového školení v oblasti kybernetické bezpečnosti.

Cíl projektu

Hlavním cílem projektu je dodání produktu, který zajistí dostatečné prostředky pro vzdělávání v oblasti kybernetické bezpečnosti jak odborných pracovníků, tak i běžných zaměstnanců.

Dílčími cíli implementace gamifikace kybernetické bezpečnosti v prostředí Správy železnic, s.o. je zejména:

- zvyšování povědomí uživatelů o kybernetických hrozbách a vytvoření podmínek pro včasnou identifikaci hrozby kybernetického útoku souvisejících s pracovní činností,
- možnost aktivně a preventivně minimalizovat možný dopad úspěšného kybernetického útoku,
- modernizovat stávající přístup k vzdělávací činnosti na základě pracovního zařazení zaměstnanců a rizikovosti dané pracovní pozice,
- splnění požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „ZKB") a vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (dále jen „VKB"),
- splnění požadavků nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 (dále jen GDPR),
- splnění požadavků zákona č. 110/2019 Sb. o zpracování osobních údajů,
- soulad s normou ISO/IEC 27001:2013.

Předběžné požadavky na řešení

- kompletní cloudové řešení (SaaS služba),
- responzivní web design řešení pro zobrazení na různých zařízeních (mobil, notebook, tablet atd.),
- kompatibilita řešení s webovými prohlížeči (browser) např. Microsoft Edge, Google Chrome, Safari, Samsung Internet atd.,
- jazykové rozhraní řešení primárně v českém jazyce a možnost volby překladu základního rozhraní a vzdělávacího programu do angličtiny a případně dalších zadavatelem určených jazyků max. 5 jazyků,
- sledování aktivity uživatelů a reporting jejich výsledků,
- customizace řešení herního prostředí dle předmětu podnikaní organizace a jednotlivých uživatelů (Kancelář, Home Office, Práce s počítačem a mobilním zařízením, internet a sociální sítě), neomezeného opakování hry, výběr herní role (profilu) zaměstnanec nebo útočník,
- přihlašování pomocí jednotného přihlašování (SSO, Singl Sign-On).

Předběžná tržní konzultace ke Gamifikace kybernetické bezpečnosti – příloha č. 2

Dotazy k technickému řešení pro Gamifikaci kybernetické bezpečnosti

1. **Cloudové řešení**
   - Jakého využíváte poskytovatele cloudového řešení?
   - Je Vaše řešení poskytováno formou Software as a Service (SaaS)?
     SaaS = model distribuce softwaru, ve kterém je software poskytován jako služba prostřednictvím internetu
2. **Responzivní design řešení**
   - Má Vaše řešení plně responzivní web design, a to pro zobrazení na různých typech zařízení (mobil, notebook, tablet atd.)?
3. **Kompatibilita řešení**
   - Je Vaše řešení kompatibilní s webovými prohlížeči (nejnovější verze) např. Microsoft Edge, Google Chrome, Safari, Samsung Internet atd.?
4. **Jazykové rozhraní řešení**
   - Je jazykové rozhraní Vašeho řešení v českém jazyce?
   - Existují i další jazykové mutace Vašeho řešení?
5. **Auditovatelnost řešení**
   - Umožňuje Vaše řešení auditovat činnost uživatelů (minimálně ve formě auditu přístupu)?
   - Umožňuje Vaše řešení připojení (integraci) do nástroje Security Information and Event management?
6. **Reporting**
   - Umožňuje Vaše řešení sledovat aktivity uživatelů a jejich herních výsledků?
   - Umožňuje Vaše řešení rozdělení do modulů, které je možné plánovat a průběžně vyhodnocovat?
   - Umožňuje Vaše řešení integrace do business inteligence nástrojů?
7. **Customizace, rozvoj a údržba řešení**
   - Umožňuje Vaše řešení individuální zákaznické customizace a firemní adaptace herního prostředí, a to dle závislosti na potřebách a interní bezpečnostní legislativy organizace a jednotlivých uživatelských skupin ve smyslu vytvoření specifického herního prostředí (akcentující soutěživý charakter, stručnost, rychlost, srozumitelnost a praktické ilustrativní ukázky a zkouška situace „na vlastní kůži" herního prostředí) pro kancelářské uživatele, home office, práce s počítačem a mobilním zařízením, Internet a sociální sítě atd.?
   - Umožňuje Vaše řešení uživateli neomezené opakování hry?
   - Umožňuje Vaše řešení výběr z herních rolí, a to na příklad zaměstnanec anebo útočník?
   - Jaká je odhadovaná cena údržby a provozu Vašeho řešení za rok?
   - Jaká je cena rozvoje Vašeho řešení (cena za funkcionalitu/MD)?
8. **Uživatelský přístup k řešení**
   - Umožňuje Vaše řešení přihlašování pomocí jednotného přihlášení SSO (tzn. Singl Sign-On)?
   - Umožnuje Vaše řešení i jiné způsoby přihlašování, popřípadě uveďte jaké.
9. **Alternativy řešení**
   - Lze poskytnout proof of concept nebo demo verzi Vámi nabízeného řešení, které se významně liší (alternativní řešení) od současných vzdělávacích softwarových nástrojů a přístupů k problematice vzdělávání kybernetické bezpečnosti jako je např.:
     - Learning Management System (LMS) nebo Enterprise Learning Management System (ELMS) - Moodle, Blackboard, Unifor, Canvas, Talent atp.
     - Learning Experience Platform (LXP) – Thrive, Cornestone atp.
     - Course Management System (CMS) – Elmo, EdApp, Showbie atp.
     - Online vzdělávací portály – Seduo, Edunio, Eduardo, Udemy atp.
10. **Implementace řešení**

- Jaké jsou minimální požadavky (funkční/technické) na součinnost (implementaci) z Vaší strany nebo ze strany dodavatele Vašeho řešení?
- Jaká je průměrná doba implementace Vašeho řešení, a to na základě Vaších zkušeností a s ohledem na velikost Správy železnic, s.o.?

11. Harmonogram řešení

- Můžete dle poskytnutého popisu PTK sestavit indikativní harmonogram implementace Vašeho řešení včetně součinností?

12. Nativní řešení

- Jsou výše uvedené customizace (funkcionality) atd. součástí Vašeho řešení nebo bude nutné některé funkcionality plně customizovat a vytvářet na míru Zadavateli? Pokud ano, jaké?

13. Prostředí

- Je níže uvedený popis prostředí a informace pro návrh Vašeho řešení dostačující? Pokud ne, jaké informace zde postrádáte?

Licenční model a podmínky

- 5 999 uživatelů,
- 2 administrátoři,
- 2 správci systému.

Potřebné informace pro návrh Vašeho řešení

1. Plánovaný počet uživatelů ~5 999.
   Pozn. Počet zaměstnanců se v čase dynamicky mění a nelze s přesností určit počet koncových uživatelů poptávaného řešení.
2. Podpora poptávaného řešení na dobu tří let.
   Pozn. Součástí podpory je školení poptávaného řešení pro administrátory.
3. Součástí poptávaného řešení není nákup hardware.

Základní popis ICT prostředí Správy železnic, státní organizace (dále též jen „SŽ" nebo „Správa železnic")

Níže uvedený popis slouží pro základní přehledné seznámení potenciálním dodavatelům o současném ICT prostředí SŽ.

ICT Prostředí SŽ obsahuje:

1. Architektonické principy SŽ.
2. Katalog služeb SŽ.
3. Katalog technologií SŽ.

Pozn. Při plánování a rozšiřování ICT řešení je nutné respektovat všechny části popisu prostředí SŽ. V případech zakázkového vývoje software pro SŽ musí dodavatel splnit požadavky definované v dokumentu Standardy vývoje informačních systémů SŽ, dokument je dostupný na vyžádání.

1. Architektonické principy

Základní rámec pravidel a principů, které je nutné respektovat při návrhu a realizaci ICT řešení v prostředí SŽ.

P01: Bezpečnost a soulad s vnitropodnikovými předpisy:

- Navrhované řešení a procesy jím podporované musí být v souladu s legislativními a regulatorními nároky a vnitropodnikovými předpisy Správy železnic.

- Řešení musí umožnit monitorování akcí uživatelů, zejména jejich práce s daty a dokumenty.
- Musí být zajištěna administrovatelnost a auditovatelnost integračních vazeb.
- Vývoj a test není realizován na produkčním prostředí.
- Topologie a architektura produkčního a testovacího prostředí musí být identická, odlišovat se může ve výkonu a použitých zdrojích.
- Před nasazením do produkčního prostředí je řešení prokazatelně otestováno.
- Nejsou realizovány integrace mezi produkčními a neprodukčními prostředími.
- Dohled je zajištěn na všech vrstvách řešení (HW, OS, DB, AS, aplikace, koncový uživatel).
- Musí být zajištěno napojení na centrální dohledovou konzoli.
- Služby poskytované do prostředí internetu budou procházet penetračním testem.

Zdůvodnění: Bezpečnost umožňuje chránit hodnoty Správy železnic. V SŽ je nutné udržovat vysokou míru bezpečnosti, a to především v oblastech, které mohou mít dopady na lidské životy. Navrhovaná řešení také musí být nezbytně v souladu s Vyhláškou č. 82/2018 Sb. o kybernetické bezpečnosti.

P02: Provozovatelnost řešení:

- Řešení je provozovatelné na službách a technologiích Správy železnic.
- Řešení musí umožňovat převzetí do provozního prostředí Správy železnic.
- Řešení umožňuje škálování.

Zdůvodnění: Z důvodu snahy o udržitelnost provozu je stanoven udržitelný počet technologií, které jsou spolehlivé a mají perspektivu svého rozvoje. Aplikace provozovaná na takto definované skupině technologií tak může být v případě potřeby převzata do provozu a spravována týmem IT specialistů SŽ, jenž disponuje patřičnými znalostmi, případně vlastní příslušné certifikace, aby mohli tyto technologie či systémy spravovat. Tím dochází nejen ke zvýšení produktivity, ale také k časové a finanční úspoře, především z pohledu lidských zdrojů.

P03: Znovu použitelnost řešení:

- Řešení musí umožňovat logické oddělení dat pro současné využívání funkcionality různými subjekty (tzv. multitenant).
- V rámci Správy železnic se realizuje minimalizace počtu a rozsahu používaných technologií a aplikací.
- Snižováním počtu a rozsahu používaných technologií a aplikací snižujeme komplexitu správy technologického a aplikačního portfolia.
- Řešení je navrhované s opakováním ověřených jednoduchých návrhových vzorů a designových principů.
- Nasazování změn a nových řešení je seskupováno dle funkcionalit a cílových systémů do jednotlivých „release". Termíny release jsou stanoveny organizační jednotkou SŽ Správa železniční telematiky (dále též „SŽT").
- Nasazované řešení nesmí ke svému provozu vyžadovat pravidelný nutný zásah administrátora (např. restarty, čištění logů, ...).

Zdůvodnění: V rámci Správy železnic usilujeme o minimalizaci počtu prostředí pro stejnou funkcionalitu. Znovupoužitelná řešení vedou k úspoře lidských, finančních, časových i materiálních zdrojů v životním cyklu celého řešení.

P04: Nezávislost na dodavatelích:

- Řešení je navrhované s ohledem na omezení či eliminaci rizika vendor-lock.
- U řešení převzatých do provozu je cíl převzetí schopnosti vytvořit build aplikace bez závislosti na dodavateli.
- Usilujeme o právo zásahu do zdrojových kódů a rozvoje řešení interními kapacitami Správy železnic nebo dalšími dodavateli. Výjimku mohou tvořit jen případy, kdy by takové požadavky byly ekonomicky výrazně nevýhodné nebo je důvod se domnívat, že tato práva budou nadbytečná.

Zdůvodnění: Nebýt závislí na malém počtu dodavatelů umožňuje SŽ být transparentní a flexibilní. Vyšší míra flexibility je také výhodná pro vyjednávaní s jednotlivými dodavateli o ekonomických a technických podmínkách.

P05: Nákup a vývoj:

- U nákupu standardizovaných komerčních produktů je požadována schopnost nastavení balíkového řešení interními kapacitami či nezávislými externími dodavateli.
- U standardizovaných agend je preferován nákup a úprava před zakázkovým vývojem nového zákaznického řešení.
- Vzájemné integrace musí být realizované přes aplikační middleware. Integrační scénáře zajišťují, aby implementace nových funkcí v řídící aplikaci minimalizovala vyvolané změny na straně návazných aplikací.
- Preferujeme přírůstkovou integraci před přenosem kompletních informací.
- Preferujeme řešení v min. třívrstvé či vícevrstvé architektuře s min. oddělením databázové, aplikační a prezentační vrstvy.
- Minimalizujeme dodávku řešení s takovými úpravami, které by omezovaly nebo eliminovaly přechod na budoucí vyšší verze produktu.
- V transakčních systémech preferujeme pouze základní operativní reporting. Plný reporting je implementovaný v analytických nástrojích.
- Řešení je řádně dokumentované po stránce vývojové, provozní a uživatelské.
- Případné zdrojové kódy jsou verzovány a ověřeny, že z nich je možno vytvořit interními týmy Správy železnic build aplikace. Zdrojové kódy a dokumentace jsou ukládány na standardizované úložiště Správy železnic.
- Návrh prostředí reflektuje trendy technologií a zároveň business potřeby.

Zdůvodnění: Regulace nákupu a do-vývoje integrací a aplikací slouží k co nejsrozumitelnějšímu a transparentnímu užívání daných technologií. Díky danému postupu v nákupu a vývoji je možné se efektivně vyrovnat s novinkami, které nově nakoupené produkty představují.

P06: Business kontinuita jako zásadní činnost:

- Navržené řešení musí odpovídat kritičnosti aplikace a požadovaným parametrům SLA.
- Servisní model a parametry aplikace odpovídají bezpečnostní klasifikaci a byznysové kritičnosti aplikace.
- Dle servisního modelu jsou definované plány obnovy a „disaster recovery" postupy.

Zdůvodnění: Správa železnic jakožto správce železniční dopravní cesty, kritické infrastruktury státu, musí být připraven na případné narušení provozu, a proto musí požadovat taková řešení, která umožní zajistit kontinuitu a obnovu klíčových procesů, činností a systémů organizace.

2. Služby SŽ

Tato kapitola popisuje seznam ICT služeb a jednotlivých HW/SW komponent, které tvoří standard v rámci Správy železnic. Cílem je zajistit ve fázích přípravy poptávky, návrhu ICT řešení a realizace dodávky kompatibilitu se stávajícím ICT prostředím a v maximální míře využít již provozované komponenty a technologie. Seznam služeb a komponent je průběžně aktualizován.

ICT služby jsou rozděleny do následujících skupin (kategorií):

- **Infrastrukturní**
  Infrastrukturní službou je míněno poskytování IT infrastruktury na úrovni HW, virtualizace, operačních systémů a diskových úložišť.

- **Platformní**
  Platformní služba poskytuje databázovou platformu či portálové řešení, které integruje webové aplikace a služby do jednoho spolupracujícího celku. Podporuje standardizované komunikační protokoly a formáty dat.

- **Podpůrné**
  Podpůrné služby zajišťují komplexní správu a provoz IT infrastruktury. Například monitorovací systémy, zálohování, reporting. Podpůrné služby jsou povinné k využití dodavatelem, pokud není jinak určeno SŽ.

Infrastrukturní služby SŽ

Služba virtuálních strojů

Služba virtuálních strojů (dále jen „VM“) je provozována na vysoce dostupné virtualizační technologii VMware a hardware s procesory Intel Xeon E5-26XX, Intel Silver 4215. Všechna VM s operačním systémem Windows Server mají nainstalován balík VMware Open Tool.

Parametry služby jako sizing virtuálních strojů, výběr OS podporovaných SŽ, počet a konfigurace síťových karet jsou konfigurovány individuálně na základě požadavků projektu, resp. dodávaného řešení.

SŽ zajišťuje vysokou dostupnost služby virtuálních strojů na úrovni vi, a to v rámci jednoho datového centra. Pokud služby dodávaného řešení vyžadují zajištění vysoké dostupnosti, tato musí být zajištěna dodavatelem v rámci dodávky včetně služby loadbalancingu.

Služba	Popis
Win.VMware.x86_64	Služby virtuálního serveru s operačním systémem Windows Server na virtualizaci VMware a architektuře x86_64
RHEL.VMware.x86_64	Služby virtuálního serveru s operačním systémem RHEL (RedHat Enterprise Linux) na virtualizaci VMware a architektuře x86_64
SLES.VMware.x86_64	Služby virtuálního serveru s operačním systémem SLES (SUSE Linux Enterprise Server) na virtualizaci VMware a architektuře x86_64 Omezení: Využití výhradně pro SAP

Služba datového uložiště

Služba datového úložiště je provozována na datových úložištích typu SAN, která jsou osazena 10K SAS disky v RAID 5 (+hotspare disk) případně RAID 6, nebo disky SSD v RAID 5 (+hotspare disk) pro aplikace vyžadující vyšší výkon, typicky databáze. V rámci služby datového uložiště není poskytována služba replikace mezi SAN úložišti, ani služba tieringu. V primárním datovém centru CDP je dále provozováno škálovatelné, výkonné, softwarově-definované datové uložiště postavené na technologii VMware vSAN, využívající prostředků fyzických serverů x86 a jejich komponent (cpu, ram, nic a disk). VMware vSAN je nativně integrované s hypervisorem VMware ESXi.

Služba	Popis
Lokální datový disk 10K	Služba datového úložiště, provozovaného na SAN storage a 10K discích v RAID 5 (+hotspare) případně RAID 6 poli, pro systémové a datové disky
Lokální datový disk SSD	Služba datového úložiště, provozovaného na SAN storage osazeného SSD disky v poli RAID 5 (+hotspare)

Platformní služby SŽ

Platformní služba (PaaS – Platform as a Service) poskytuje databázovou či integrační platformu (middleware). Tato integruje aplikace a služby do jednoho spolupracujícího celku. Podporuje standardizované komunikační protokoly a formáty dat.

V rámci platformy Správy železnic jsou poskytovány tyto platformní služby:

Služba zabezpečeného portálového řešení

Služba	Popis
Liferay na VMware.x86_64	Liferay je přední open-source podnikové portálové řešení založené na jazyce Java, které umožňuje správu dat, aplikací, procesů a integrace současných i nových aplikací z jednoho centrálního uživatelského rozhraní.

Služba zabezpečených webových serverů

Služba	Popis
Microsoft IIS na Win.VMware.x86_64	Služba webového serveru postavená na technologií Microsoft Internet Information Services (IIS) provozovaná na serverech s operačním systémem Windows Server s virtualizací VMware.
Apache HTTP Server na Win.VMware.x86_64	Služba webového serveru postavená na open-source technologii Apache provozovaná na serverech s operačním systémem Windows Server s virtualizací VMware.
Apache HTTP Server na RHEL.VMware.x86_64	Služba webového serveru postavená na open-source technologii Apache provozovaná na serverech s operačním systémem RHEL s virtualizací VMware.

Služby zabezpečených aplikačních serverů

Služba	Popis
.NET na Win.VMware.x86_64	Aplikační server Microsoft .NET prostředí pro vývoj a provoz aplikací založených na .NET frameworku
JBOSS na Win.VMware.x86_64	Služba virtuálního aplikačního serveru JBOSS provozovaná na serverech s operačním systémem Windows Server s virtualizací VMware.
Oracle WebLogic na RHEL.VMware.x86_64	Služba virtuálního aplikačního Oracle WebLogic Serveru (WLS), pro provoz aplikací postavených na standardu JAVA EE na serverech s operačním systémem RHEL s virtualizací VMware.
Oracle WebLogic na SLES.VMware.x86_64	Služba virtuálního aplikačního Oracle WebLogic Serveru (WLS), pro provoz aplikací postavených na standardu JAVA EE na serverech s operačním systémem SLES s virtualizací VMware.
Oracle WebLogic na Win.VMware.x86_64	Služba virtuálního aplikačního Oracle WebLogic Serveru (WLS), pro provoz aplikací postavených na standardu JAVA EE na serverech s operačním systémem Windows Server s virtualizací VMware.

Služby zabezpečených databázových prostředí

Služba	Popis
Oracle DB na Oracle Exadata	Databázová služba Oracle DB provozovaná na optimalizovaném hardware Oracle Exadata Database Machine – kombinovaná hardwarová a softwarová platforma.
MS SQL na Win.VMware.x86_64	Služba virtuálních databázových serverů MS SQL Server provozovaná na serverech s operačním systémem Windows Server a virtualizační platformě VMware.

Podpůrné služby SŽ

Podpůrné služby standardně poskytované k využití pro dodávaná ICT řešení

Bezpečnost

Služby zabezpečení infrastruktury

Služba	Popis
Antivirus	Antivirové řešení fSecure, provozované jako virtualní appliance, zajišťuje ochranu koncových stanic a serverové infrastruktury před škodlivým obsahem, zejména malwarem, exploity, síťovými útoky a jinými bezpečnostními hrozbami. Každé datové centrum Správy železnic disponuje vlastní virtuální appliance fSecure. Nasazením antivirového řešení fSecure jako virtuální appliance, jsou minimalizovány konzumované výpočetní zdroje a dopad na výkon virtualizační infrastruktury.
PAM	Privileged Access Management (PAM) je řešení které pomáhá kontrolovat, monitorovat, zabezpečit a auditovat privilegované identity před jejich zneužitím. **Omezení**: Aktuálně v pilotním provozu
IDM	Identity Management (IDM) je řešení umožňující řízení uživatelských účtů a jejich oprávnění napříč systémy. IDM umožňuje lepší přehlednost, bezpečnost a automatizaci. V prostředí Správy železnic bylo implementováno open-source řešení MidPoint společnosti Evolveum, jenž nevyžaduje nákup licencí. Toto řešení má otevřenou a rozšiřitelnou architekturu založenou na standardech Java, XML a REST.
Active Directory and Domain Services	Adresářová služba společnosti Microsoft pro správu zařízení a identit a jejich autentizaci a autorizaci v podnikových sítích. Dodávaná řešení musí podporovat integraci na službu Active Directory Správy železnic. Správa železnic provozuje multi-forest prostředí, proto musí aplikace umožňovat využití více AD konektorů, za účelem ověření uživatelů.

Monitoring, alerting

Služba	Popis
Monitoring	
Zabbix	Služba dohledu infrastruktury je zajištěna pomocí dohledových agentů instalovaných na provozovaném prostředí nebo bez-agentově se vzdáleným dohledem, sledování standardními protokoly SNMP, HTTP, HTTPS apod. Dodavatelé ve spolupráci s jednotkou SŽT zajistí napojení dodávaných řešení na monitoring Zadavatele. Tím není dotčena případná povinnost dodavatele řešení monitorovat kvalitu a dostupnost dodávaného řešení v rámci vlastního monitoringu.

Aktualizace systémů, Distribuce aplikací

Služba	Popis
Aktualizace	
Distribuce SW a aktualizace koncových stanic	Technologií System Center Configuration Manager (SCCM) je zajištěna distribuce softwarových balíčků a aktualizace koncových

	stanic. Patchování klientských stanic probíhá 1 x měsíčně a je plně v gesci Správy železnic.
Aktualizace serverových operačních systémů	Aktualizace serverových operačních systému Windows Server je řešena skriptovacím jazykem Powershell. Patchování serverových operačních systémů probíhá 1 x měsíčně a je zajištěno Správou železnic, pokud není s dodavatelem řešení dohodnuto jinak. Aktualizace serverových operačních systémů založených na linuxové distribuci je prováděna manuálně, na vyžádání správce aplikace, nebo v reakci na kybernetické hrozby.

Zálohování

Služba	Popis
Zálohování a obnova	Služba zálohování prostředí je zajištěna technologií IBM Spectrum Protect (TSM – Tivoli Storage Manager) komplexním řešením pro fyzické fileservery, virtualizované prostředí a širokou škálu aplikací. IBM Spectrum Protect zálohuje data s využitím technologie VMware snapshot. Služba zálohování umožňuje 3 základní typy zálohování: Snapshot disku pro dosažení rychlé obnovy celého OS v Crash Consistent stavu včetně aplikační konfigurace. Zpravidla je takto zálohován pouze systémový oddíl virtualizovaného serveru. Záloha probíhá jednou denně a retence je nastavena na 30 posledních verzí. Záloha datových svazků připojených k jednotlivým serverům, pro dosažení max. možné odolnosti proti náhodnému smazání či poškození apod. Záloha probíhá jednou denně, kdy se uchovává 90 posledních verzí souborů a poslední smazaná verze souboru je uchovávána 365 dní. Zálohy Oracle nebo SQL databází pomocí agentů. Záloha probíhá dvakrát denně. Přes den jsou zálohovány transakční logy databází, v noci pak vlastní databáze. Retence je nastavena na 60 posledních verzí.

Komunikační infrastruktura

Služba	Popis
DNS	Domain Name System (DNS) je kritickou službou, která má zásadní vliv na bezpečnost, odezvu a dostupnost služeb SŽ. Je nezbytná pro správný chod podnikové sítě a služeb na bázi Active directory. Správa železnic provozuje interní i externí službu DNS.
Firewall	Firewall soustava je velmi důležitým uzlem veškeré komunikace v síti SŽ, jenž pomocí pravidel filtruje síťový provoz a chrání prostředky v síti Správy železnic.
Proxy	Proxy soustava zajišťuje přístup uživatelů a serverů k internetu. Naprostá většina komunikace uživatelů do internetu prochází přes ni, jiný přístup není povolen. Proxy servery fungují jako prostředník mezi klienty a cílovými servery, mimo perimetr sítě SŽ, překládá klientské požadavky a vůči cílovému serveru vystupuje sám jako klient.
Reverzní proxy	Všechna připojení z internetu směřující na některý ze serverů jsou směrována přes reverzní proxy server, který buďto požadavek zpracuje sám nebo ho předá dál serverům. Umožňuje SSL terminaci a kompresi.
VPN	Služba virtuální privátní sítě, umožňující dodavateli zabezpečený přístup k prostředkům datových center Správy železnic.
VPN S2S	Služba virtuální privátní sítě Site-to-Site.

3. Technologie SŽ

Níže uvedené popisuje technologie, jež tvoří základ k výše uvedeným infrastrukturním a platformním službám.

Tyto softwarové a hardwarové prostředky nesmějí být přímo použity v návrhu řešení. Jejich použití je možné pouze prostřednictvím výše uvedených infrastrukturních nebo platformních služeb.

Pro některé případy výběrových řízení pro aplikační software je přípustné použití tzv. zapouzdřených technologií, jež nejsou součástí ICT prostředí SŽ, ale nabízené řešení vyžaduje jejich nasazení.

Zapouzdřená technologie je zpravidla součástí jiné primární technologie jako tzv. podpůrný program. Takový program nevyžaduje samostatnou instalaci, jelikož je instalován jako součást dané komponenty.

Použití takových zapouzdřených technologií je možné jen v následujících případech:

1. Jejich použití nebude klást žádné dodatečné provozní, finanční ani implementační nároky po celou dobu životnosti primární technologie.
2. Nebudou vyžadovat žádné dodatečné licence nad rámec licencí hlavního dodávaného řešení.
3. Aktualizace zapouzdřených technologií bude probíhat pouze současně s aktualizací hlavního dodávaného řešení.
4. Jejich podpora bude poskytována současně a ve stejném rozsahu jako podpora hlavního dodávaného řešení.
5. Zapouzdřené technologie nebudou vyžadovat žádné speciální provozní či bezpečnostní zajištění.

Při použití zapouzdřených technologií je nutné danou technologii identifikovat nejméně v následujícím rozsahu:

- název,
- verze,
- výrobce,
- licence,
- termín a úroveň podpory.

Technologie	Popis
Integrace	
LifeRay	Bezplatný open-source podnikový portál založený na jazyce Java, umožňující správu dat, aplikací a procesů.
Aplikační servery	
Microsoft Internet Information Services (IIS)	Framework pro běh třívrstvých podnikových aplikací s kolekcí rozšiřujících modulů provozovaný nad operačními systémy Windows, vytvořený společností Microsoft.
Oracle WebLogic Server	Aplikační server Oracle WebLogic Server (WLS) pro provoz aplikací na platformě J2EE.
JBoss	Aplikační server JBoss pro provoz platformy J2EE pro řešení s potřebou autonomního prostředí, nebo pro aplikace nepožadující vysokou dostupnost.
Webové servery	
Apache HTTP Server	Webový server postavený na open-source technologii Apache.

MS IIS	Webový server s kolekcí rozšiřujících modulů provozovaný nad operačními systémy Windows, vytvořený společností Microsoft.
Databázové systémy	
Oracle Database	Relační databázový systém společnosti Oracle určený pro mission critical aplikace.
Microsoft SQL	Relační a analytický databázový systém Microsoft SQL Server.
Serverové operační systémy	
Windows Server	Operační systém, na němž jsou provozovány aplikační či webové služby a databázové stroje založené zejména na technologiích společnosti Microsoft.
RHEL	Operační systém RedHat Enterprise Linux (RHEL) je linuxová distribuce společnosti RedHat určená pro komerční sféru. Použití pro aplikační servery.
SLES	Operační systém SUSE Linux Enterprise Server (SLES) je linuxová distribuce společnosti SUSE určená pro komerční sféru. Použití pro aplikační servery.
Virtualizační platformy	
VMware	Primární virtualizační platforma pro virtualizaci hardwarové platformy x86_64. Tato zajišťuje business kontinuitu, škálovatelnost a flexibilitu provozu pro operační systémy. Platforma je primárně určena pro virtualizaci operačních systému Windows, případně Linux.
Oracle VM	Virtualizační platforma Oracle, pro virtualizaci hardwarové platformy x86_64 založena na technologii Citrix Xen Hypervisor. Omezené využití: Primárně určena pro provoz Oracle DB.
Hardware	
x86_64	Servery postavené na architektuře x86_64 – 64bitové procesory, provozovány na platformě Intel 2-socketových serverech typu rack a blade.
SAN datová uložiště	Uložiště dat s podporou vysoké dostupnosti, škálování a vysokou úrovní zabezpečení. Podporuje vytváření snapshotů, replikaci dat a automatický tiering datových uložišť.
Network and Security	
VPN	Zabezpečený vzdálený přístup do sítě SŽ je řešen pomocí technologie Cisco ASA.
Firewall	Zabezpečení pomocí firewall pravidel je zabezpečeno technologií Cisco.