

Váš dopis zn.
Ze dne
Naše zn. 73750/2022-SŽ-GŘ-O8
Listů/příloh 3/1

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

Datum 24. říjen 2022

Pozvánka k předběžné tržní konzultaci ve věci přípravy zadávacích podmínek na veřejnou zakázku s názvem „Log Management“

Vážená paní, vážený pane,

Správa železnic, státní organizace (dále jen „Zadavatel“) Vás touto cestou informuje o tom, že připravuje zadávací řízení na veřejnou zakázku „Log Management“. Vyhlášení této veřejné zakázky bude předcházet předběžná tržní konzultace (dále jen „PTK“), jejímž cílem bude získat relevantní informace pro správné nastavení předmětu plnění, zadávacích podmínek, volby druhu zadávacího řízení a způsobu hodnocení předložených nabídek. Zadavatel usiluje o získání kvalitního plnění, které bude splňovat jeho potřeby, a to za odpovídající cenu.

Zadavatel jako subjekt povinný v souladu s ustanoveními § 3 písm. c), d), ve znění § 2 písm. e) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (dále také „ZoKB“), je na základě platného Plánu zvládnání rizik v oblasti kybernetické bezpečnosti zavázána provádět bezpečnostní opatření (viz § 5 ZoKB) pro zajištění kybernetické bezpečnosti informačních a komunikačních systémů spravovaných Zadavatelem. Konsolidace sběru provozních a bezpečnostních logů ze systémů a sítě Zadavatele je jedním ze způsobů, jak naplnit tyto povinnosti.

Jako technické opatření k naplnění výše uvedeného se Zadavatel připravuje k realizaci implementace systému pro zajištění Log Managementu. Tento Log Management zajistí sběr, zpracování, dlouhodobé zaručené ukládání, umožní analyzovat a dlouhodobě ukládat záznamy o událostech v komponentách, systémech a aplikacích Zadavatele tak, aby byly prokazatelné, chráněné a udržované v souladu se zákonnými požadavky.

Log Management bude implementován v prostředí Zadavatele, které tvoří velmi rozsáhlá a komplikovaná ICT infrastruktura rozmístěná v lokalitách rozprostřených po celém území České republiky.

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 č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „Zákon“) možností zadavatele předtím, než vyhlásí veřejnou zakázku, přičemž zadavatel má možnost v rámci PTK komunikovat s dodavatelem (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.

Forma předběžné tržní konzultace: písemná (s možností pokračování ústní formou)

V rámci PTK žádáme o zodpovězení dotazů zadavatele uvedených v příloze č. 1 této pozvánky. Odpovědi, které obdrží Zadavatel budou pečlivě analyzovány a vyhodnoceny. S ohledem na účel PTK Zadavatel přihledne 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 „Log Management“. Zadavatel o dalším průběhu PTK osloví vždy minimálně ty dodavatele, kteří projevíli zájem o PTK v předcházejícím kole.

V případě Vašeho zájmu o účast na této PTK zašlete své odpovědi na otázky uvedené v příloze č. 1 této pozvánky na emailovou adresu: hemzova@spravazeleznic.cz. **Svoji odpověď prosím doručte nejpozději do 7. 11. 2022.**

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:

Jméno osoby: **Miriam Hemzová**
email: **Hemzova@spravazeleznic.cz**

Zadavatel sděluje, že připravovaná veřejná zakázka je plánována k zadání jako nadlimitní sektorová veřejná zakázka.

Předpokládaný počátek plnění předmětu veřejné zakázky je 2. polovina 2023. Předpokládaná délka trvání veřejné zakázky je 12 měsíců, přičemž tato délka může být na základě realizované PTK upravena.

PTK nesmí vést k porušení základních zásad Zákona. Průběh i výsledek PTK proto bude zaznamenán ve zprávě vytvořené Zadavatelem. Informace z PTK užití v zadávacích podmínkách veřejné zakázky budou v souladu s § 36 odst. 4 Zákona v zadávací dokumentaci výslovně označeny, 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 organizační jednotky
Správa železničních informačních technologií

Přílohy:
Příloha 1 – Otázky pro písemnou část PTK

Předběžná tržní konzultace – Log Management – Příloha 1

Dotazy k technickému řešení pro Log Management

1. Centrální vs. decentralizovaný sběr logů

- Uvedte, které z uvedených variant přístupu k řešení sběru logů podporuje vaše řešení.
- Uvedte klíčová kritéria pro rozhodnutí, která varianta je vhodná v jakých situacích.
- Popište vrcholovou architekturu pro všechny vámi podporované varianty řešení.

2. Transport logů od zdrojů logů (Log Sources) do Log Managementu

- Uvedte, zda a jak vaše řešení přímo podporuje zajištění kompletního přenosu logů od zdroje až k místu pro vyhodnocování logů.
- Uvedte doporučení, zda je vhodné, aby si Zadavatel realizoval transportní vrstvu interními silami. Jaké jsou výhody a nevýhody takového přístupu?
- Jaké jsou možnosti využití vašeho řešení v případě, že se Zadavatel snaží vyhnout vendor lock-inu prostřednictvím oddělení transportní vrstvy?

3. Vztah řešení Log Management a SIEM (Security Information and Event Management)

- Pokud zadavatel plánuje budoucí nasazení řešení SIEM, je vhodné spojit takovou aktivitu s realizací řešení Log managementu? Jaké jsou výhody doporučeného přístupu?
- V případě, že vaše řešení poskytuje také funkcionality SIEM, popište je (příp. je poskytněte formou přílohy k vaší odpovědi v českém nebo anglickém jazyce).
- Jaké podmínky pro hladké nasazení SIEM by měl podle vás Zadavatel zajistit v případě odděleného nasazení LM a SIEM?

4. Použití Log Management řešení pro více kontextů, např. zvlášť pro IT (Information Technology) a OT (Operational Technology)

- Uvedte klíčová kritéria pro rozhodnutí, v jakých situacích je vhodné oddělit Log Management pro IT/OT a jaké z toho mohou plynout důsledky pro architekturu řešení.
- Popište vrcholovou architekturu pro obě varianty.

5. Provoz řešení v režimu Multi-Tenant

- Uvedte, zda vaše řešení podporuje fungování v režimu Multi-Tenant, tedy s podporou bezpečné identifikace zdrojových logů různých subjektů, jejich bezpečný přenos, izolované uložení a výslednou interpretaci řízenou dle patřičných přístupových oprávnění.
- Popište, zda uvažované řešení umožňuje fungování v prostředích, která mají kolizní některé atributy logujících aktiv:
 - a. IP adresace
 - b. jmenné konvence aktiv
 - c. uživatelské identifikace

Licenční model a podmínky

Popište licenční model a licenční podmínky platné pro všechny součásti řešení.

Potřebné informace pro návrh a nacenění nabídek k budoucí veřejné zakázce

Uvedte, jaké jsou potřebné informace, které by Zadavatel měl uvést v rámci zadávací dokumentace tak, aby budoucí uchazeči mohli sestavit svou nabídku včetně nabídkové ceny za poptávané plnění. V případě, že pro tento účel využíváte formuláře pro sběr potřebných dat, prosíme o jejich přiložení k odpovědi.