STÁTNÍ POZEMKOVÝ ÚŘAD

VÝZVA K ÚČASTI NA PŘEDBĚŽNÉ TRŽNÍ KONZULTACI K VEŘEJNÉ ZAKÁZCE NA DODÁVKU SYSTÉMU PRO CENTRÁLNÍ SPRÁVU LOGŮ

ZADAVATEL:

Zadavatel:	**Česká republika – Státní pozemkový úřad**
Sídlo:	Husinecká 1024/11a, 130 00 Praha 3 - Žižkov
Zastoupený:	Ing. Martinem Vrbou, ústředním ředitelem
Kontaktní osoba	Ing. Monika Mrkvičková, odbor.zakazky@spucr.cz
IČO / DIČ	01312774 / CZ 01312774
Internetová adresa profilu zadavatele:	**https://zakazky.spucr.cz/**
ID Datové schránky:	z49per3
Č.j. / Spis. zn.:	SPU 446191/2019

Státní pozemkový úřad tímto vyzývá potenciální dodavatele k účasti na předběžné tržní konzultaci (dále také „PTK“), která se bude konat v průběhu měsíce listopadu a prosince.

Místo konání: Státní pozemkový úřad, Husinecká 1024/11a, 130 00 Praha 3 - Žižkov

Zájemci se mohou registrovat na e-mailové adrese: odbor.zakazky@spucr.cz
Termín registrace: do 24. 11. 2019
V registraci zájemci uvedou:

1) název a IČO dodavatele
2) jména osob, které se zúčastní PTK (lze dodatečně změnit či upřesnit)
3) do předmětu e-mailu uvedou „PTK – Centrální správa logů“.

Každý zaregistrovaný dodavatel obdrží pozvánku na konkrétní den a hodinu, a to po předchozí domluvě.

1. ÚVOD

Česká republika – Státní pozemkový úřad (dále také „SPÚ“) připravuje zadávací řízení na veřejnou zakázku na dodávku systému pro centrální správu logů pro Státní pozemkový úřad (dále jen „CSL“).

Před zahájením zadávacího řízení se zadavatel rozhodl využít institutu PTK dle ust. § 33 zákona č. 134/2016 Sb., ve znění pozdějších předpisů, o zadávání veřejných zakázek (dále jen „zákon“), jako nástroje ke komunikaci s dodavateli, a to za účelem zjištění relevantních a objektivních informací o možnostech daného trhu.

Cílem PTK je připravit zadávací podmínky vč. řádného definování a ověření specifikace předmětu plnění, tak aby nejlépe vyhovoval potřebám zadavatele a současně možnostem trhu; prověřit si u dodavatelů eventuality řešení požadavků zadavatele na funkcionality předmětu plnění, získat zpětnou vazbu daného řešení či existenci jiných možností CSL.

Aktivní účast v PTK nemá vliv na následnou účast v zadávacím řízení. PTK nesmí narušit hospodářskou soutěž a nesmí vést k porušení zásady zákazu diskriminace a zásady transparentnosti postupu zadavatele. Průběh a výsledek PTK bude zaznamenán v samostatné zprávě, která bude součástí zadávacích podmínek veřejné zakázky.

2. CÍL VEŘEJNÉ ZAKÁZKY

Cílem veřejné zakázky je

1) zajištění CSL vyhovujícího legislativním požadavkům (Zákon o kybernetické bezpečnosti a ČSN ISO 27001 pro pořizování auditních záznamů apod.)
2) zajištění CSL schopného provozu ve vysoké dostupnosti zajišťující kontinuitu sběru a zpracování logů
3) zajištění CSL, které provádí zpracování událostí ze zdrojů logů (aktivní síťové prvky, servery, koncové stanice, aplikace) napříč výrobci aplikací, OS a HW s možností rozšíření o podporu dalších zařízení a systému, tak aby byl použitelný pro systémy a zařízení provozované na SPÚ a to i v budoucnu;
4) zajištění podpory CSL, a to jak HW tak SW části, na dobu minimálně 5 let včetně zajištění aktualizací všech částí systémů a parserů zdrojů logů;

3. FORMA A PRŮBĚH PŘEDBĚŽNÉ TRŽNÍ KONZULTACE

Účast na PTK je otevřená. Účastnit se jí mohou zejména všichni potenciální zájemci o předmětnou veřejnou zakázku (dále jen „dodavatelé“). V rámci zvýšení informovanosti o zahájení PTK zadavatel současně adresně oslovil několik konkrétních dodavatelů (viz bod 4).

PTK bude probíhat formou individuálních pohovorů, z jednání bude pořizován audiozáznam, který bude sloužit pouze pro potřeby zadavatele. Výsledek PTK bude shrnut v zápisu, který bude uveřejněn na profilu zadavatele SPÚ.

V rámci PTK bude zadavatel s dodavateli konzultovat zejména návrhy na možná řešení uložení písemností SPÚ v rámci komplexního zajištění poskytovaných služeb, navržený způsob hodnocení, předpokládanou hodnotu apod. Podklady pro PTK jsou obsaženy v souborech, které jsou na profilu zadavatele uveřejněny spolu s touto výzvou. Jedná se především o návrh Požadavků zadavatele na předmět zakázky včetně příloh.

4. OSLOVENÍ DODAVATELÉ

Zadavatel dopisem ze dne 8. 11. 2019 adresně upozornil na zahájení PTK níže uvedené dodavatele:

1) CompuNet s.r.o., IČO 27608514, Štefánikova 13/43, 150 00 Praha-Smíchov, compunet@compunet.cz
2) COMGUARD a.s,, IČO 04305426, Freyova 27, 190 00 Praha 9, e-mail: praha@comguard.cz

3) DATASYS s.r.o., IČO 61249157, Jeseniova 2829/20, 130 00 Praha 3, e-mail: datasys@datasys.cz
4) Auriga Systems s.r.o., IČO 28871235, Naardenská 671/6, 162 00 Praha 6, , e-mail: obchod@aurigasystems.cz,
5) PCS spol. s r. o., IČO 00571024, divize DataGuard, Na Dvorcích 18, 140 00 Praha 4, e-mail: dataguard@pcs.cz,
6) AUTOCONT a.s., IČO 04308697, Hornopolní 3322/34, 702 00 Ostrava, e-mail: obchod@autocont.cz

5. POPIS STÁVAJÍCÍHO STAVU

SPÚ je správním úřadem s celostátní působností provozující v současné době dva významné informační systémy dle vyhlášky č. 317/2014 Sb. a další systémy v souladu s požadavky zákona o kybernetické bezpečnosti.
CSL je v současnosti zajištěna systémem LOGmanager od výrobce Sirwisa a. s., který plní funkci SEM (Security Event Management) – centralizovaná správa událostí a logů. Tento systém byl pořízen v roce 2015 a na konci roku 2020 bude tedy na konci životnosti a bez smluvně zajištění podpory.
Systém LOGmanager implementovaný na SPÚ se skládá ze dvou zařízení (appliance) pracujících v režimu vysoké dostupnosti. Aktuálně platná legislativa požaduje uchování dat po dobu minimálně dvanácti měsíců, ale současný systém s kapacitou cca 30 TB umožnuje uchovat data maximálně po dobu čtyř měsíců. Aktuálně systém zpracovává průměrně cca 4000 událostí za sekundu, což je cca polovina výkonnostní kapacity.
Vedení SPÚ rozhodlo na základě analýzy rizik a legislativních požadavků o zajištění nového CSL, která by odpovídal aktuálním legislativním požadavkům (zejména zákonu č. 181/2014 Sb., o kybernetické bezpečnosti, vyhlášce č. 317/2014 Sb., o významných informačních systémech, vyhlášce č. 82/2018, o kybernetické bezpečnosti a GDPR), normám (ČSN/ISO 27001) a moderním trendům v oblasti centrální správy logů.

Základní údaje o zadavateli

Název zadavatele: **Česká republika – Státní pozemkový úřad**

Právní forma: služební úřad v rámci organizační složky státu MZe ČR

Počet krajských pracovišť: 13

Počet poboček: 64

6. POPIS POŽADOVANÉHO STAVU CSL

- CSL vyhovující aktuálním legislativním požadavkům (zejména zákonu č. 181/2014 Sb., o kybernetické bezpečnosti, vyhlášce č. 317/2014 Sb., o významných informačních systémech, vyhlášce č. 82/2018, o kybernetické bezpečnosti a GDPR), normám (ČSN/ISO 27001) a moderním trendům v oblasti centrální správy logů;
- CSL zajišťující konsolidaci logů na jednom centrálním místě
- CSL schopný provozu ve vysoké dostupnosti zajišťující kontinuitu sběru a zpracování logů

- CSL pracující jako appliance nebo obdobné řešení, které není výkonově závislé na prostředí objednatele
- CSL, které provádí zpracování událostí ze zdrojů logů (aktivní síťové prvky, servery, koncové stanice, aplikace) napříč výrobci aplikací, OS (především MS Windows) a HW (minimální seznam podporovaných zdrojů logů v příloze č. 1) s možností rozšíření o podporu dalších zařízení a systému, tak aby byl použitelný pro systémy a zařízení provozované na SPÚ a to i v budoucnu;
- CSL s dostatečnou kapacitou pro uchování logů po dobu 12ti měsíců (SPÚ provozuje cca 170 serverů (včetně virtuálních), 1500 koncových stanic (PC, NTB), 5 diskových polí, 150 switchů a zařízení pro provoz WiFi (centrální i pobočkové), 80 firewallů a IPS (centrální i pobočkové), a asi 120 aplikací (monitorováno bude jen cca 10 nejdůležitějších), odhadovaná datová zátěž 250 – 350 GB zdrojových dat denně;
- CSL s dostatečným výkonem pro zpracování zdrojů dat i s výhledem do budoucna (předpoklad cca 10 000 událostí za sekundu);
- CSL s možností kapacitní i výkonové škálovatelnosti a rozšiřitelnosti v případě růstu datové zátěže logy v budoucnosti
- CSL se zajištěnou podporou, a to jak HW tak SW části na dobu minimálně 5 let včetně zajištění aktualizací všech částí systémů a parserů zdrojů logů;
- Přijaté logy CSL standardizuje do jednotného formátu, logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu a zároveň systém uchovává i originální verzi zpráv tak, aby bylo možné výsledky předávat k případné další analýze dalším orgánům (NÚKIB, PČR, apod.);
- Správa CSL je řešena jedním uceleným rozhraním pro všechny administrátorské i operátorské činnosti bez nutnosti dodatečného programování pro vyhledávání událostí;
- CSL je schopen na základě zadaných podmínek splněných v přijatých datech vygenerovat alert;
- CSL musí obsahovat řešení, které sbírá události na pobočkách a umožní jejich odeslání v šifrované podobě po saturované lince bez ztráty dat;
- V případě přetížení CSL nesmí dojít ke ztrátě logů.

7. TÉMATA PTK

V rámci PTK bychom chtěli potenciálním dodavatelům nabídnout možnost vyjádřit se k níže uvedeným tématům a otázkám:

a) Soulad řešení CSL s legislativními požadavky a normami
Konkrétní řešení jednotlivých legislativních požadavků a norem vyjmenovaných v popisu požadovaném stavu CSL.

b) Řešení jednotlivých požadavků z popisu požadovaného stavu CSL
Konkrétní řešení jednotlivých požadavků z popisu požadovaném stavu CSL (provozní, výkonnostní a kapacitní parametry).

c) **HW vs. SW řešení vs. Cloud řešení**
Vhodná řešení splňující požadavky SPÚ založená pracující jako HW+SW, SW, Appliance či v Cloudu – porovnání, výhody a nevýhody jednotlivých řešení (provozní, cenové, apod.). Skladba a výše cen jednotlivých typů rešení.

d) **Škálovatelnost a rozšiřitelnost**
Jak nabízené řešení řeší požadavek na škálovatelnost a rozšiřitelnost do budoucna (výkonovou, kapacitní, funkční – nové parsery, apod.)?

e) **SEM vs SIEM**
Vhodnost omezit nabízené řešení pouze na SEM (legislativní požadavek) či rovnou poptávat SIEM z pohledu možnosti nabízených řešení na trhu a jejich ceny.

f) **Výkonnost řešení**
Jaké jsou výkonnosti vámi nabízených řešení (příjem a zpracování událostí za sekundu, odezvy při prohledávání logů v závislosti na složitosti dotazu)?

g) **Rozhraní pro správu CSL**
Prezentace jednotného a uceleného rozhraní pro správu nabízených řešení CSL tak, aby bylo zřejmé že splňuje požadavky na přehlednost, jednotnost a bezpečnost (granularita oprávnění, autentizace a autorizace, apod,). Lokalizace do českého jazyka? Technické požadavky na provoz tohoto rozhraní.

h) **Implementace**
Stručný bodový postup implementace a nasazení nabízených řešení, principiální požadavky na součinnost.

i) **Personální a kvalifikační předpoklady**
Disponují Vaši zaměstnanci a nabízená řešení certifikace či jiná osvědčení prokazující splnění zejména legislativních požadavků a norem, případně jakých?

j) **Zkušenosti s nasazením obdobných řešení ve státní správě**
Žádáme, abyste rozvedli své zkušenosti v rámci nasazení nabízených řešení ve státní správě. Můžete předložit přehled a reference v posledních 4 letech?

k) **Možnosti hodnocení VZ**
Jak si představujete optimální hodnocení VZ? Hodnocení na nejnižší nabídkovou cenu či nějaká další vhodná váhová kritéria?

Diskuze nad konkrétními tématy bude vedena v rámci osobního rozhovoru s každým účastníkem PTK samostatně.

Do té doby uvítáme Vaši zpětnou vazbu k uvedeným tématům, případně zaslání nových podnětů nebo otázek, které by bylo vhodné projednat v rámci PTK. Návrhy je možné zasílat na níže uvedenou adresu, a to i v případě, že se dodavatel PTK účastnit nebude.

Vaše případné podněty, návrhy či okruhy k jednání nám, prosím, posílejte do 24. 11. 2019 na e-mailovou adresu **odbor.zakazky@spucr.cz**, do předmětu e-mailu uveďte: „**PTK – Centrální správa logů**“.

Případné další informace o formě a průběhu PTK i další související dokumenty budou uveřejňovány na profilu zadavatele na adrese: https://zakazky.spucr.cz/vz00026899
a budou o nich informováni všichni dodavatelé, kteří projeví zájem účastnit se PTK.

V Praze dne 6. 11. 2019

……
Mgr. Pavel Škeřík
ředitel Sekce provozních činností

v z. Ing. Lenka Tůmová

Příloha:
Příloha č. 1 – Minimální seznam podporovaných zdrojů logů