Vysvětlení zadávací dokumentace č. 5

IDENTIFIKAČNÍ ÚDAJE ZADAVATELE

Název veřejného zadavatele:	Středočeský kraj
Sídlo zadavatele:	Zborovská 81/11, 150 21 Praha 5 - Smíchov
IČO zadavatele:	70891095
Osoba oprávněná jednat za zadavatele:	Mgr. Petra Pecková, hejtmanka Středočeského kraje
Profil zadavatele:	https://zakazky.kr-stredocesky.cz/

zastoupen na základě plné moci

Zmocněnec:	ARROWS advokátní kancelář, s.r.o.
Sídlo zmocněnce:	Plzeňská 3350/18, Smíchov, 150 00 Praha 5
IČ zmocněnce:	06717586
Kontaktní osoba:	Mgr. Antonín Hajdušek. LL.M., advokát
Elektronická adresa:	hajdusek@arws.cz
Telefonní kontakt:	+420 725 992 682

Zmocněnec je pověřen výkonem zadavatelských činností dle § 43 zákona na základě plné moci

NÁZEV A DRUH ZAKÁZKY

Název veřejné zakázky	**Zajištění kybernetické bezpečnosti informačních systémů krajského úřadu – dohledové centrum SOC**
Druh veřejné zakázky	služby

Ve smyslu ust. § 98 odst. 3 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění (dále jen „***zákon***“), obdržel zadavatel dne 21. 8. 2024 a 22. 8. 2024 níže uvedené dotazy s žádostí o vysvětlení případně úpravu zadávací dokumentace k výše uvedené veřejné zakázce.

Zadavatel tímto prostřednictvím zmocněné osoby zastupující zadavatele poskytuje níže vysvětlení zadávací dokumentace k této veřejné zakázce na základě položených dotazů:

Znění žádostí o vysvětlení zadávací dokumentace:

1. Pro určení výkonnosti sond pro “Analýza datových toků a detekce bezpečnostních událostí” žádáme dodavatele o definici požadovaného výkonu. Předpokládáme, že je požadovaný kompletní monitoring – všech paketů. V případě některých řešení sond může být limitní objem monitoringu u hranice 0,5M pps. Jaký nyní bývá špičkový provoz z pohledu paketů za sekundu. Resp. v jaké max. hodnotě požaduje zadavatel garantovat zajištění monitoringu pro špičkový provoz z pohledu paketů za sekundu pro poskytování monitoringu po dobu poskytování služby?

Odpověď zadavatele:
Špičkový provoz dosahuje průměrně 900.000 paketů/s. S ohledem na budoucí vývoj a historické hodnoty špičkového provozu je nutný minimální výkon pro monitorovací sondy alespoň 1,35 milionu paketů/s na každém jednom portu.

2. Dotaz k Zadávací dokumentaci „příloha č. 1 Zadávací dokumentace „Technická specifikace“ a limitaci poddodavatele ve smyslu čl. 11 zadavatele

1. V příloze č. 1 Zadávací dokumentace „Technická specifikace“ zadavatel požaduje mimo jiné splnění následujícího požadavku uváděného v **kapitole 1.3. přílohy č. 1 Zadávací dokumentace (*„Dohledové centrum – SOC“*)**:

„Poskytovatel prokazatelně doloží, že provozuje CSIRT (CERT), který je registrovaný v databázi TF – CSIRT Trusted Introducer – úroveň Accredited nebo vyšší / anebo ***u jiné obdobné organizace zabývající se bezpečnostními incidenty a reakcemi*** *na ně,* ***přičemž registrace u těchto organizací potvrzuje schopnost poskytovatele reagovat na bezpečnostní incidenty a spolupracovat s dalšími CSIRTy a potvrzuje schopnost poskytovatele poskytovat kvalitní služby, a to vše na úrovní srovnatelné alespoň s úrovni Accredited v rámci databáze TF – CSIRT Trusted Introducer****."*

2. Zadavatel současně v čl. 11 zadávací dokumentace stanoví následující:

   11.1. Zadavatel v souladu s § 105 odst. 2 zákona požaduje, ***aby následující významné činnosti při plnění veřejné zakázky byly plněny přímo vybraným dodavatelem, tj. nikoliv prostřednictvím poddodavatelů****:*

   - dohledové centrum – SOC.

   11.2. Dodavatel ve své nabídce specifikuje části veřejné zakázky, které má v úmyslu zadat jednomu či více poddodavatelům, a uvede identifikační údaje každého poddodavatele. Dodavatel závazně využije přílohu č. 6 zadávací dokumentace – Seznam poddodavatelů. V případě, že dodavateli nejsou známi poddodavatelé, jež se budou podílet na plnění veřejné zakázky, tabulku nevyplňuje (tento dokument ale i tak dodavatel předloží v rámci své nabídky).

3. Vlastní předmět veřejné zakázky se skládá ve smyslu Přílohy č. 1, konkrétně kapitoly 1 této přílohy, zadávací dokumentace z plnění pro následující oblasti, resp. celky:

   Záměrem zadavatele je nakoupit služby zařazené do 3 celků:

   1. ***Sdílené služby kybernetické bezpečnosti*** *– Jedná se o komplexní dodávku dílčích služeb po dobu 60 měsíců:*

   1.1. Zaznamenávání a ukládání logů a detekce bezpečnostních událostí – Dodavatel s využitím vlastních technologií zajistí sběr, ukládání, analýzu a bezpečné dlouhodobé uchování logů z vybraných systémů IT zadavatele. Současné dodavatel zajistí detekci bezpečnostních událostí v sledovaných systémech IT dodavatele a informování o nich.

   1.2. Analýza datových toků a detekce bezpečnostních událostí – Dodavatel s využitím vlastních technologií zajistí sledování datových toků na výskyt anomálií a podezřelých aktivit a měření výkonových parametrů datových přenosů v síti IT zadavatele. Současně dodavatel zajistí záznam a uložení informací o sledovaných datových tocích, detekovaných událostech a stavech a o výsledcích měření sledovaných veličin.

   1.3. Dohledové centrum – SOC – Dodavatel s využitím vlastních zdrojů zajistí provoz Bezpečnostního dohledového centra, které pro zadavatele bude provádět bezpečnostní dohled nad sledovanými systémy IT, identifikaci, hodnocení a řešení bezpečnostních incidentů včetně poskytnutí včasných informací odpovědným pracovníkům zadavatele, pravidelné reportování stavu kybernetické bezpečnosti sledovaných systémů IT a poskytování podpory v oblasti kybernetické bezpečnosti.

   2. ***Audit kybernetické bezpečnosti*** *– Jedná se o zajištění auditní činnosti vyplývající z Vyhlášky dle § 16 – Audit kybernetické bezpečnosti, každý uvedený bod bude realizován v průběhu trvání veřejné zakázky, vždy po dohodě se zadavatelem.*

   2.1. Penetrační testování vybrané webové aplikace – Dodavatel provede penetrační test vybraných webových aplikací po dohodě se zadavatelem. Testování bude prováděno formou gray box, dle standardu OWASP. Hodnocení provést pomocí hodnotícího systému NIST CVSSv3 (nebo vyšší). 2.2. Penetrační testování perimetru – Dodavatel provede penetrační testování perimetru. Testování bude prováděno formou gray box. Test bude proveden prostřednictvím simulace útoku na vybrané informační systémy Zadavatele.

   2.3. Penetrační testování vnitřního systému – Dodavatel provede penetrační testování vnitřní infrastruktury. Testování bude prováděno formou gray box.

   3. ***Služby poradenství a podpory*** *– Jedná se o komplexní dodávku dílčích služeb, které směřují ke koordinaci a kvalitnímu provedení dodávky ostatních služeb:*

3.1. *Předimplementační analýza – Dodavatel zpracuje analýzu prostředí IT kraje, ve které popíše a vyhodnotí stav z hlediska zajištění kybernetické bezpečnosti podle §16, §17, §18, §22, §23, §24 a §27 Vyhlášky, identifikuje bezpečnostní rizika a slabá místa a navrhne opatření k odstranění neshod.*

3.2. *Prováděcí dokumentace – Dodavatel zpracuje prováděcí dokumentaci s detailním návrhem cílového stavu, s popisem aktivit potřebných pro řádnou implementaci jednotlivých služeb včetně implementace opatření navržených v předimplementační analýze a s návrhem harmonogramu implementačních prací. Součástí dokumentace bude také popis potřebných integrací do prostředí IT kraje.*

3.3. *Projektové vedení dodávky – Dodavatel zajistí řízení, koordinaci a dokumentaci postupu dodávky včetně řízení rizik a změn dodávky a poskytování pravidelných zpráv o průběhu dodávky.*

3.4. *Dokumentace skutečného provedení – Dodavatel v průběhu celé dodávky zajistí zpracování dokumentace dodaných řešení v požadovaném rozsahu.*

Služby v rámci celku „*Sdílené služby kybernetické bezpečnosti*“ představují klíčovou a rozhodnout část plnění, která v sobě zahrnuje služby spojené s vytvořením *„Dohledového centra – SOC“.*

Jak pak vyplývá z předchozích odpovědí k žádostem o vysvětlení zadávací dokumentace Zadavatel trvá na požadavku na akreditaci u TF-CSIRT Trusted Introducer nebo obdobné organizace (viz vysvětlení č. 4 k zadávací dokumentaci).

Stanovení výhrady dle § 105 odst. 2 z.č. 134/2016 Sb. o zadávání veřejných zakázek (dále jen „ZZVZ“) však nesmí být takové, že by zcela znemožnilo dodavatelům prokázat chybějící kvalifikace jinou osobou. V daném případě a ve světle technické kvalifikace ve smyslu § 79 odst. 2 písm. b) ZZVZ (viz čl. 6.3.1.1. zadávací dokumentace) je však z povahy věci možnost využít poddodavatele pro plnění „dohledové centrum – SOC“ zcela vyloučena.

Požadavek na akreditaci u dotčené organizace, příp. jiných obdobných organizací představuje požadavek ve spojení s požadovanou technickou kvalifikací a úplném vyloučení poddodavatelů pro nejpodstatnější část plnění veřejné zakázky zcela bezdůvodnou překážku hospodářské soutěže ve smyslu § 36 odst. 1 z.č. 134/2016 Sb. o zadávání veřejných zakázek (dále jen „ZZVZ“).

Ve světle shora uvedeného bychom se rádi dotázali, zdali zadavatel umožní dodavatelům využití poddodavatele pro prokázání kvalifikace dle čl. 6.3.1.1. zadávací dokumentace?

V opačném případě žádáme Zadavatele o objektivní a relevantní zdůvodnění, proč právě pro poskytování této části plnění vylučuje možnost využití služeb poddodavatele.

Odpověď zadavatele:

Zadavatel předně uvádí, že má povinnosti vyplývající ze zákona o kybernetické bezpečnosti, přičemž jednou z nich je právě sběr logů, vyhodnocování a ukládání po dobu 12 měsíců. Zadavatel přitom není schopen vlastními silami této povinnosti dostát (zejm. personální a technologické důvody), proto plnění těchto povinností řeší zajištěním externí služby spočívající mimo jiné i v poskytnutí služby dohledového centra – SOC.

Jedná se tedy o významnou a zcela zásadní činnost v rámci plnění předmětné veřejné zakázky a zadavatel tak zcela v souladu s ust. § 105 odst. 2 ZZVZ stanovil, že tato činnost při plnění veřejné zakázky musí být plněna přímo vybraným dodavatelem. Účelem této výhrady je tedy získat zvýšenou kontrolu nad poskytováním služby a dohled nad zásadními částmi plnění veřejné zakázky.

Zadavatel pak souhlasí, že z výše uvedených důvodů tak není možné prokázat kritérium technické kvalifikace podle čl. 6.3.1 poddodavatelem. Tato skutečnost tak plyne z výhrady zadavatele, aby dohledové centrum – SOC, coby významná činnost při plnění veřejné zakázky, byla plněna přímo vybraným dodavatelem.

Výše uvedený postup a důsledek nemožnosti prokázat kritérium technické kvalifikace podle čl. 6.3.1 zadávací dokumentace je však zcela v souladu se zákonem o zadávání veřejných zakázek, a zadavatel proto odmítá, že by se jednalo, jak uvádí dodavatel, o zcela bezdůvodnou překážku hospodářské soutěže ve smyslu § 36 odst. 1 ZZVZ.

Zadavatel pak uzavírá, že na jednu stranu jsou sice dodavatelé dle § 83 ZZVZ oprávněni prokázat část kvalifikace prostřednictvím jiných osob, na druhou stranu mají zadavatelé právo toto oprávnění fakticky omezit využitím výhrady podle § 105 odst. 2 ZZVZ. Aby se oprávnění dodavatelů dle § 83 ZZVZ nestalo obsoletním, je samozřejmě třeba trvat na tom, aby zadavatelé i z tohoto důvodu právo podle § 105 odst. 2 ZZVZ vykonávali v přiměřeném rozsahu a z objektivních důvodů. Zadavatel má však za to, že s ohledem na zcela zásadní a významnou část plnění veřejné zakázky, kterou dohledové centrum SOC představuje, těmto limitům dostál a své právo uplatňuje v přiměřeném rozsahu a z objektivních důvodů.

V Praze dne 23. 8. 2024

Mgr. Antonín Hajdušek, LL.M., advokát
ARROWS advokátní kancelář, s.r.o.,
zastupující zadavatele na základě plné moci

Mgr.
Antonín
Hajdušek

Digitálně podepsal Mgr. Antonín Hajdušek
DN: c=CZ, 2.5.4.97=NTRCZ-06717586, o=ARROWS advokátní kancelář, s.r.o., ou=2, cn=Mgr. Antonín Hajdušek, sn=Hajdušek, givenName=Antonín, serialNumber=P331691
Datum: 2024.08.23 15:24:06 +02'00'