

Vysvětlení zadávací dokumentace č. 4

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 12. 8. 2024 a 13. 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. V „Příloze 1- Technická specifikace předmětu zakázky“ se v tabulkách vyplňuje odpověď ANO/NE. V případě odpovědi „NE“ jedná se o vyřazovací kritérium?

Odpověď zadavatele:

Ano, v případě odpovědi „NE“ jde o nesplnění technických podmínek vymezujících předmět veřejné zakázky, které podle ust. § 37 odst. 1 písm. b) zákona představují podmínky účasti v zadávacím řízení.

2. V „Příloze 1 – Technická specifikace předmětu zakázky“ V bodě **1.2 Analýza datových toků a detekce bezpečnostních událostí** je toto znění:

Realizace tohoto opatření naplní § 23 Detekce kybernetických bezpečnostních událostí Vyhlášky.

Jedná se o komplexní službu pro monitorování sítě KÚSK na základě datových toků, kterou umožní nástroje pro sledování provozu a zabezpečení sítě. Služba bude podporovat následná řešení vyskytujících se problémů a nestandardních stavů v síti, monitoring aktivit uživatelů a provozovaných SW aplikací. Služba umožní správcům pohled na využití síťového provozu na infrastruktuře KÚSK. Služba disponuje funkcí, která umožní sledovat výkonové parametry sítě a technologií

analýzy datových toků včetně vyhodnocování chování sítě v návaznosti na aktuální hrozby a nestandardní stavy. Rozsahy a formy poskytovaných rozšiřujících služeb nesmí být pevně svázána s rozsahem a formou poskytované služby SOC. Nabízené rozšíření služby SOC zajistí provozování celého systému tak, aby odpovídal všem relevantním zákonným normám a aktuálním trendům v dané oblasti a zadavatel nemusel investovat do dalších lidských zdrojů pro administraci, správu a podporu řešení.

Požadovaný účel služby:

Poskytnout komplexní službu pro zaznamenávání aplikačních logů vznikajících na infrastruktuře KÚSK s důrazem na autonomní detekci bezpečnostních událostí v oblasti provozovaných VIS KÚSK na serverové části včetně možnosti jejich uložení do neměnné databáze. Zajistit poskytování služby dodavatelem v souladu s požadavky zadavatele a trendy v oboru.

DOTAZ: Po zaslání informací po podepsání NDA V následné tabulce jsou vypsány požadavky, ze kterých si nejsme jisti, zda se jedná o načítání dat nebo i dodávku nového řešení. Prosíme o upřesnění, zda předmětem je i dodávka a zprovoznění nových síťových sond, nebo zda se jedná o monitoring a sběr logů ze stávajících zařízení, která byla definována.

Odpověď zadavatele:

Aktuálně používané sondy nejsou v majetku Krajského úřadu Středočeského kraje, ale jsou součástí poskytované služby. S ohledem na jejich stáří bude nutná obměna.

3. V „Příloze 1- Technická specifikace předmětu zakázky“ v tabulce v bodě 1.3 Dohledové centrum – SOC jsou následující požadavky:

	POŽADAVEK	OTÁZKA
5.	Reporty systému budou sloužit pro přehlednou kontrolu stavu a chování informačních systémů a uživatelů za určité období (typicky 1 měsíc) a ke kontrole dodržování compliance („jednání v souladu s pravidly“) organizace zadavatele.	Předpokládáme, že report se bude týkat bezpečnostního stavu a chování. Je tomu tak?
12.	Součástí dodávky bude návrh změn konfigurací dotčených a souvisejících systémů, koordinace provedení změn s provozovateli systémů a ověření správné konfigurace.	Co je myšleno pod koordinací provedení změn? Toto není úloha SOC, ale Zadavatele. Nebo se jedná o koordinaci v rámci Zadavatele a Dodavatele a ne třetích stran?
14.	Průběžné monitorování IT prvků dodaných v rámci této veřejné zakázky, popř. prvků IT, které mohou ovlivnit jejich chod. Počet sledovaných parametrů nesmí být prakticky omezen (min. stovky).	V rámci dodávané služby předpokládáme, že SOC řeší bezpečnostní monitoring. Provozní monitoring řeší Zadavatel. Je tomu tak?
15.	Monitoring bude probíhat minimálně dle výstupů ze služby pro zaznamenávání a ukládání logů a detekce bezpečnostních událostí (SIEM), systému analýzy datových toků a detekce bezpečnostních událostí,	Opět chápeme jako bezpečnostní monitoring, je tomu tak?
	systému pro pokročilý provozní dohled a firewallů zadavatele.	

17.	<p>Rozšířený monitoring a specifické služby provozního zajištění komodity SOC:</p> <ul style="list-style-type: none"> (r) Provádění monitoringu systému a zpracovávaných dat v rozsahu potřebném pro provádění následujících služeb. (s) Informování odpovědných osob zadavatele o vzniku bezpečnostního incidentu v reálném čase za pomoci základních komunikačních nástrojů (mail / SMS / tel). (t) Zahájení řešení bezpečnostního incidentu do 4 hodin od vzniku, řízení souvisejících činností správců a případných dalších dotčených osob. (u) Zakládání tiketů, proaktivní komunikace o jejich řešení. Komunikace s třetí stranou jako NBÚ, NUKIB, CSIRT atd. (v) Rozšířený reporting – detailní report o událostech a incidentech s návrhy systematických opatření 1x měsíčně. Vzdálená prezentace reportu např. formou videokonference. (w) Kontinuální skenování aktiv definovaných danou sítí/sítěmi a zranitelností relevantních pro daná aktiva. Minimálně na začátku poskytování služby budou provedeny plné skeny a dále vždy 1x měsíčně skeny rozdílové. (x) Přístup administrátorů zadavatele ke sledovaným parametrům alespoň v režimu čtení prostřednictvím grafického rozhraní (GUI – dashboard apod.). 	<p>U bodu „T“ předpokládáme, že incident management není součástí služby a není tedy naceněn, ale lze jej v případě potřeby využít? V bodě „W“ - Vlastníte SW na skenování zranitelností nebo má být poskytnut v rámci služby? Případně jaký SW Zadavatel vlastní? Co je myšleno sledovanými parametry v bodě „X“?</p>
22.	<p>Služba Monitoring a detekce - Zajištění Operátorské úrovně Průběžné sledování provozu prostředí objednatele. Real-time analýza situace v napojených zařízeních podle skupin, kategorií zařízení a podle kontextu log záznamů nebo událostí. Posouzení kontextu anomálie a příčin vzniku situace s případnou eskalací problému objednatele na analytického specialistu dodavatele.</p>	<p>Služba by měla zastřešovat sledování bezpečnostního provozu Zadavatele. Je tomu tak?</p>

Odpověď zadavatele:

Ad 5)	ano
Ad 12)	ano, jedná se o koordinaci v rámci Zadavatel a Dodavatel
Ad 14)	ano
Ad 15)	ano

Ad 17)	u bodu T ano, k bodu W – Zadavatel má k dispozici sledování zranitelností pracovních stanic, u ostatních síťových prvků a serverů tomu tak není, bod X – je tím myšlen přístup administrátorů k výstupům z monitoringu v režimu čtení
Ad 22)	ano

4. V bodě 2.2. je požadavek na detailní popis zajištění bezpečnosti informací. - co je tím myšleno? Je to v rámci prováděné implementace?

Odpověď zadavatele:

Ano je to v rámci prováděné implementace.

5. Obecné dotazy týkající se penetračních testů:

- Je umožněna možnost využití automatických nástrojů (pokud ano máte na ně nějaké podmínky/omezení)?
- Jsou nějaké požadované časy testování (předpokládáme 9:00-17:00 v pracovní dny). Je požadování provádět testy o víkendech, svátcích, apod.?
- Máte specifické podmínky na reporting (předpokládáme využití vlastních šablon pro závěrečné zprávy)?

Odpověď zadavatele:

Používání automatizovaných nástrojů je možné po dohodě se Zadavatelem před zahájením testů. Obvykle požaduje testování v pracovních dnech od 09.00 hod do 17.00 hod. Je možné ale po předchozí domluvě využít i dnů pracovního volna. Pro závěrečné zprávy je možné využít šablon Dodavatele.

6. Lze poskytnout plánec nebo popis současné infrastruktury co se týče primárních a podpůrných aktiv, které by se napojovali do SIEM řešení?

Odpověď zadavatele:

S ohledem na citlivost dat lze poskytnout pouze obecné informace. Bližší popis lze poskytnout pouze v režimu po podpisu NDA.

7. Kolik bezpečnostních událostí se v současné době řeší (týdně/měsíčně)?

Odpověď zadavatele:

Průměrně zadavatel řeší 30 událostí měsíčně bez další klasifikace. Do uvedeného počtu se počítají i false positive události.

8. Zadavatel v odst. 5.11 obchodních podmínek (smlouva o dílo – dále jen „obchodní podmínky“) požaduje, aby v případě součástí díla, které jsou předmětem ochrany práv podle autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), v platném znění, poskytl zadavateli územně, časově i množstevně neomezenou výhradní převoditelnou licenci.

Řešení, kterým dodavatel disponuje, je standardizovanou službou, jejíchž součástí je celá řada předmětů práv podle autorského zákona, a dodavatel tak nemůže udělit zadavateli výhradní licenci k nim. Sám zadavatel v obchodních podmínkách poměrně nešťastně formuluje, že předmětem díla je služba. Dle názoru dodavatele není předmětem veřejné zakázky dílo podle § 2586 občanského zákoníku, ale předmětem plnění je poskytování služeb. Z předmětu plnění nijak nevyplývá, že snad zadavatel očekává vybudování vlastního systému „na zelené louce“, ke kterému by následně mohl zadavatel získat výhradní licence. Tomu neodpovídá ani předpokládaná hodnota, která by pro výhradní vybudování takového systému na míru musela být násobně dražší. Dodavatel žádá, aby zadavatel nepožadoval nevýhradní licenci a upravil obchodní podmínky tak, aby dodavatel mohl při poskytování služeb používat standardní software, který si řídí licenčními podmínkami výrobců, kteří zpravidla udělování neomezených licencí neumožňují.

S tím souvisí i následující odst. 5.12, pro který platí stejné skutečnosti, které dodavatel již uvedl. K žádnému faktickému předání díla nedochází (budou pouze poskytovány služby), a k řešení, které dodavatel nabízí, rozhodně nemůže být zadavateli uděleno oprávnění takové řešení rozmnožovat, překládat, zpracovávat, upravovat či jinak měnit nebo nechat měnit, spojit s jiným dílem, jakož i zařazovat do díla souborného, a získaná oprávnění postupovat zcela nebo zčásti třetí osobě, v souladu s jeho účelem a určením vč. provádění oprav vad díla objednatel nebo prostřednictvím jiných osob.

Zadavatel se rozhodně na základě veřejné zakázky nestane neomezeným výhradním uživatelem žádného díla, jelikož k vytvoření žádného díla pro něj na zakázku nedochází. Nebude tak ani předáván žádný zdrojový kód.

Na základě výše uvedeného dodavatel žádá, aby zadavatel z obchodních podmínek předmětné odst. 5.11 – 5.19 odstranil.

Odpověď zadavatele:

Zadavatel uvádí, že požadavek dodavatele je důvodný a zadavatel se proto rozhodl předmětná ujednání podle čl. V odst. 5 až 11 z obchodních podmínek odstranit.

Za tímto účelem zadavatel přikládá k tomuto Vysvětlení zadávací dokumentace jako přílohu č. 1 upravené znění obchodních podmínek (návrhu smlouvy o dílo), ve kterém jsou ujednání dle čl. V odst. 11 – 19 návrhu smlouvy odstraněny. Takto upravené znění obchodních podmínek přitom zcela nahrazuje původně poskytnuté, coby příloha č. 3 zadávací dokumentace.

9. Zadavatel v technické specifikaci předmětu zakázky uvádí, že dodavatelé, kteří se budou podílet na rozvoji, provozu nebo zajištění bezpečnosti významných informačních systémů, musí dle § 8 VKB, splňovat bezpečnostní požadavky pro dodavatele. Zadavatel ovšem neuvádí, jaké bezpečnostní požadavky pro dodavatele si podle § 8 odst. 1 písm. a). VKB stanovil. Dodavatel tak neví, jaká pravidla má konkrétně dodržovat. Může zadavatel specifikovat?

Odpověď zadavatele:

Zadavatel coby přílohu č. 2 tohoto Vysvětlení zadávací dokumentace uveřejňuje dokument „Politika řízení dodavatelů“, který tvoří přílohu pokyny ředitele Krajského úřadu Středočeského kraje o informační a kybernetické bezpečnosti Krajského úřadu Středočeského kraje. Tento dokument přitom obsahuje pravidla pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací podle § 8 odst. 1 písm. a) VKB.

10. Zadavatel v technické specifikaci požaduje řešení „Analýza datových toků a detekce bezpečnostních událostí“ 2 kusy sondy, které mají být „Realizováno hardware komponentami s instalací do 19“ racku, každá sonda max. 1RU. (možná SW varianta)“.

S ohledem na předpokládaný objem provozu je zřejmé, že při SW variantě sond bude při implementaci potřeba velký rozsah integrace virtualizačními prostředími zadavatele. Pokud budeme uvažovat provoz v rozsahu přesahujícím 0,75M pps, tak SW řešení vyžadují mimo jiného i dedikované přístupy k HW síťovým kartám, o kterých se nikde v ZD zadavatel nezmiňuje. Předpokládáme, že je požadovaný kompletní monitoring všech paketů. V případě některých SW řešení sond může být limitní objem monitoringu už u hranice 0,5M pps. Vzhledem k detailně popsaným požadavkům na HW sondy zadavatelem a přihlédnutí k výše uvedenému, jedná se zde o překlep a závorka (možná SW varianta), v této části ZD být neměla? Pokud ano, prosíme o její odstranění.

Odpověď zadavatele:

Zadavatel uvádí, že se jedná o nepřesnost technických podmínek, neboť s ohledem na provoz přichází v úvahu skutečně pouze HW sonda.

Za účelem nápravy výše uvedené nepřesnosti zadavatel přikládá k tomuto Vysvětlení zadávací dokumentace jako přílohu č. 3 upravené znění Technické specifikace předmětu zakázky, ve kterém je alternativa v podobě SW varianty odstraněna. Takto upravené znění Technické specifikace předmětu zakázky přitom zcela nahrazuje předchozí poskytnuté verze.

11. Zadavatel v rámci Vysvětlení č. 1 uvedl:

Zadavatel se po úvaze rozhodl vyhovět požadavku dodavatele a upravuje přílohu č. 1 zadávací dokumentace - Technická specifikace předmětu zakázky, a to v kapitole 1.3. Dohledové centrum – SOC, kde v prvním řádku zde uvedené tabulky zadavatel nově požaduje, aby poskytovatel prokazatelně doložil, že provozuje CSIRT (CERT) tým, 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 úrovni srovnatelné alespoň s úrovní Accredited v rámci databáze TF – CSIRT Trusted Introducer.

Jaké jiné organizace má v tomto směru Zadavatel na mysli? Jak hodlá Zadavatel porovnat úroveň Accredited nebo vyšší se zcela jinou institucí, tak aby byly tyto úrovně odpovídající? Můžete tedy Zadavatel pregnantně uvést konkrétní instituce a úroveň, kterou uzná jako rovnocennou s CSIRT Trusted Introducer – úroveň Accredited ?

Odpověď zadavatele:

Zadavatel demonstrativně uvádí výčet organizací a úrovní, které uzná jako rovnocenné s úrovní Accredited v rámci databáze TF – CSIRT Trusted Introducer:

- FIRST (Forum of Incident Response and Security Teams) - úroveň Full Member.
- ENISA (European Union Agency for Cybersecurity) - úroveň CERT.
- CERT/CC (Computer Emergency Response Team Coordination Center) - úroveň Accredited.

12. Zadavatel ve Vysvětlení zadávací dokumentace č. 2 uvádí, že provozuje významné informační systémy dle Zákona č. 181/2014 Sb. (ZoKB). Je tudíž povinnou osobou dle tohoto zákona. V dokumentaci není uvedeno v jaké roli dle ZoKB bude vystupovat dodavatel. Je možné, že by mohl být dodavatel označen jako „významný dodavatel“?

Odpověď zadavatele:

Ano, dodavatel by mohl být označen jako „významný dodavatel“. Tato skutečnost rovněž vyplývá ze závěrů auditu NÚKIB, provedeném v roce 2024.

13. Zadavatel v rámci ZD neuvádí žádný požadavek na incident response. Proaktivní dohled a vyhodnocování událostí SOC týmu, které jsou při obdobných zakázkách vyžadovány. V jakém režimu předpokládá Zadavatel SLA reakce SOC týmu?

Odpověď zadavatele:

Zadavatel předpokládá režim 24/7.

14. Dle minulých odpovědí zadavatele žádáme ještě o upřesnění. Pochopil uchazeč správně, že se poskytovatel v období 5 let provede 1 externí penetrační test na cca 50 veřejných adres, bude provedeno testování webových aplikací v počtu 30 aplikací dle metodologie OWASP Application Security Verification Standard (ASVS) a provede 5 testů interní infrastruktury?

Odpověď zadavatele:

Ano, poskytovatel v období 5 let provede 1 externí penetrační test na cca 50 veřejných adres, bude provedeno testování webových aplikací v počtu 30 aplikací dle metodologie OWASP Application Security Verification Standard (ASVS) a provede 5 testů interní infrastruktury.

15. Z uvedeného ZD nám nebylo zřejmé, požaduje zadavatel od poskytovatele SOC služeb napojení na pokročilou analytickou kapacitu v podobě Cyber Threat Intelligence (CTI) od NÚKIB? Ponechá si zadavatel právo před podpisem smlouvy ověřit tuto skutečnost?

Odpověď zadavatele:

Ano, zadavatel předpokládá napojení na pokročilou analytickou kapacitu v podobě Cyber Threat Intelligence (CTI) od NÚKIB. Zadavatel si vyhrazuje právo na ověření této skutečnosti v rámci posouzení nabídek.

16. Požaduje zadavatel, aby byl uchazeč pro doložení jeho kompetentnosti a s přihlédnutím, že zadavatel spadá pod ZoKB, aby byl uchazeč zapsán v Katalogu cloud computingu ČR?

Odpověď zadavatele:

Ano.

17. 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 úrovni srovnatelné alespoň s úrovní Accredited v rámci databáze TF – CSIRT Trusted Introducer.“

Požadavek na akreditaci u dotčené organizace, příp. jiných obdobných organizací představuje požadavek, který svojí povahou nenaplnuje splnění vlastního předmětu veřejné zakázky, resp. se jedná o požadavek vytvářející s ohledem na povahu veřejné zakázky bezdůvodnou překážku hospodářské soutěže ve smyslu § 36 odst. 1 z.č. 134/2016 Sb. o zadávání veřejných zakázek (dále jen „ZZVZ“). Akreditace v rámci organizace Trusted Introducer představuje v zásadě jen zájmové sdružení primárně určené ke sdílení interních kontaktů. Z hlediska schopnosti splnění veřejné zakázky je rozhodující kvalita „security týmu“ ve vazbě k vybraným projektům. V tomto ohledu naše společnost disponuje mezinárodními certifikacemi nejvyšší úrovně jako je ISO27001 či ISAE3402, které se týkají právě oblasti „Service organization control“. Jinými slovy řečeno platí, že dotčenému požadavku založenému na individuálním členství či akreditaci v jedné z mnoha zájmových organizací je dána vyšší váha, resp. vyšší význam nežli mezinárodní certifikaci typu ISO.

Vlastní požadavek, navíc splnitelný na úroveň „akreditace“ tak je z našeho pohledu nepřiměřený a v rozporu s § 36 odst. 3 ZZVZ. Bude dostačující alespoň stupeň registrace v režimu "listed", příp. zcela odstranit tento požadavek z kapitoly 1.3. přílohy č. 1 zadávací dokumentace?

Odpověď zadavatele:

Zadavatel odmítá tezi dodavatele, že předmětný požadavek zadavatele svou povahou nenaplnuje splnění vlastního předmětu veřejné zakázky, resp. že se jedná o požadavek vytvářející s ohledem na povahu veřejné zakázky bezdůvodnou překážku hospodářské soutěže ve smyslu § 36 odst. 1 zákona.

Zadavatel k požadavku na akreditaci na úrovni "Accredited" nebo vyšší u organizace TF-CSIRT Trusted Introducer, případně 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 úrovni srovnatelné alespoň s úrovní Accredited v rámci databáze TF – CSIRT Trusted uvádí, že ten je odůvodněn snahou zadavatele zajistit co nejvyšší úroveň bezpečnosti a kvality při řešení bezpečnostních incidentů. Tato akreditace není jen formalitou, ale potvrzuje, že poskytovatel splňuje přísné standardy a je schopen efektivně spolupracovat s ostatními CSIRT týmy, a to i na mezinárodní úrovni. To je klíčové pro zajištění rychlé a efektivní reakce na bezpečnostní incidenty.

Dále zadavatel odmítá rovněž názor dodavatele, že akreditace u TF-CSIRT Trusted Introducer nebo obdobné organizace je spíše otázkou zájmového sdružení, jehož účelem je sdílení kontaktů. K tomu zadavatel uvádí, že požadavek na potřebnou certifikaci/akreditaci je výrazem potvrzení, že daný tým splňuje určité technické a organizační požadavky, které jsou nezbytné pro provozování kvalitního a spolehlivého dohledového centra (SOC). Tento požadavek tedy zajišťuje, že vybraný dodavatel má nejen teoretické znalosti, ale i praktické zkušenosti a infrastrukturu potřebnou pro poskytování služeb na vysoké úrovni.

Pokud pak dodavatel uvádí, že disponuje mezinárodní certifikací jako ISO27001 nebo ISAE3402, pak zadavatel uvádí, že ty nejsou specificky zaměřeny na schopnost rychle a efektivně reagovat na bezpečnostní incidenty a spolupracovat s jinými CSIRT týmy. TF-CSIRT Trusted Introducer se zaměřuje právě na tuto oblast, a proto je tento požadavek více relevantní pro daný předmět zakázky než obecné certifikace.

V obecné rovině pak zadavatel dodává, že veřejné zakázky na IT bezpečnost mají často strategický význam a jakékoli nedostatky v kvalitě poskytovaných služeb mohou mít vážné důsledky. Proto je nezbytné klást důraz na nejvyšší standardy kvality a bezpečnosti. Požadavek na akreditaci u TF-CSIRT Trusted Introducer, případně u jiné organizace se srovnatelnou akreditací/certifikací tak slouží jako preventivní opatření proti potenciálním rizikům spojeným s nedostatečnou kvalifikací dodavatele. Zadavatel má přitom odpovědnost zajistit, že služby, které budou poskytovány, budou na nejvyšší možné úrovni, což zahrnuje i schopnost rychle a efektivně reagovat na bezpečnostní incidenty.

Zadavatel tak uzavírá, že požadavek na akreditaci u TF-CSIRT Trusted Introducer nebo obdobné organizace je nejen opodstatněný, ale i nezbytný pro zajištění maximální bezpečnosti a kvality služeb poskytovaných v rámci veřejné zakázky. Tento požadavek tedy nepředstavuje bezdůvodnou překážku hospodářské soutěže, ale spíše zajišťuje ochranu veřejných zájmů a minimalizaci rizik spojených s poskytováním kritických bezpečnostních služeb.

K požadavku dodavatele na snížení stupně registrace na režim "listed", příp. zcela odstranit požadavek z kapitoly 1.3. přílohy č. 1 zadávací dokumentace, uvádí zadavatel, že stupeň „listed“, je základní úroveň registrace v rámci Trusted Introducer. Znamená to, že organizace (CSIRT/CERT) byla uznána jako existující a funkční tým, ale neprošla žádným formálním procesem ověřování kvality a kompetencí. Na této úrovni tak není prováděna kontrola nebo audit postupů a schopností týmu. Tato úroveň tak zadavateli nestačí k prokázání potřebného standardu kvality a funkčnosti týmu. Oproti tomu "Accredited" je vyšší úroveň, která vyžaduje detailní ověření a potvrzení schopností týmu, což zadavateli poskytuje vyšší úroveň důvěry a jistoty v jeho schopnosti efektivně řešit bezpečnostní incidenty.

Z výše uvedených důvodů se tak zadavatel rozhodl požadavku dodavatele nevyhovět.

18. Zadavatel požaduje ve smyslu čl. 6.3.1. zadávací dokumentace, aby dodavatel prokázal splnění příslušné kvalifikace významnými zakázkami v následujícím rozsahu:

- a) *Alespoň 2 významné služby, jejichž předmětem bylo poskytování Sdílené služby kybernetické bezpečnosti odpovídající technické specifikaci uvedené příloze č. 1 této zadávací dokumentace. Součástí poskytování Sdílené služby kybernetické bezpečnosti mohla, ale nemusela být, i dodávka systému zaznamenávání a ukládání logů a detekce bezpečnostních událostí (SIEM - Security Information and Event Management). Minimální finanční rozsah alespoň jedné Sdílené služby kybernetické bezpečnosti na první rok provozu musel činit nejméně 2 000 000 Kč bez DPH a druhé Sdílené služby kybernetické bezpečnosti na první rok provozu nejméně 1 000 000 Kč bez DPH.*
- b) *Alespoň 2 významné služby, jejichž předmětem bylo poskytování dohledového centra SOC odpovídající technické specifikaci uvedené příloze č. 1 této zadávací dokumentace, a to v minimálním finančním rozsahu alespoň jedné služby ve výši 200 000 Kč bez DPH za měsíc a druhé služby nejméně ve výši 65 000 Kč bez DPH za měsíc. Obě tyto služby musely dohlížet na provoz prvků kritické informační infrastruktury (dle ust. § 2 písm. b) kybernetického zákona), nebo na provoz významného informačního systému spravovaného orgánem veřejné moci (dle ust. § 2 písm. d) kybernetického zákona).*

V případě významných zakázek je odkazováno na technickou specifikaci v rozsahu přílohy č. 1 zadávací dokumentace, která mimo jiné požaduje i splnění technického požadavku v rozsahu, jak uvádíme výše u dotazu č. 1 (*pozn. zadavatele: zde se jedná o dotaz č. 17*). V tomto ohledu je dotčený požadavek nepřiměřený ve vztahu k oprávněným potřebám na plnění veřejné zakázky.

Odpověď zadavatele:

S ohledem na odpověď zadavatele na dotaz č. 17 má zadavatel za to, že minimální úroveň kritéria technické kvalifikace podle čl. 6.3.1 zadávací dokumentace je stanovena přiměřeně vzhledem ke složitosti a rozsahu předmětu veřejné zakázky.

Zadavatel s ohledem na úpravy zadávacích podmínek současně v souladu s ust. § 99 odst. 2 zákona přiměřeně prodlužuje lhůtu pro podání nabídek do 4. 9. 2024 do 10:00 hodin.

Přílohy:

Příloha č. 1 – Obchodní podmínky – revize 1

Příloha č. 2 – Politika řízení dodavatelů

Příloha č. 3 - Technická specifikace předmětu zakázky – revize 3

V Praze dne 15. 8. 2024

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