Vysvětlení zadávací dokumentace č. 2

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 22. 7. 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 vyskytuje public/NDA. Předpokládáme, že pro získání podrobnějších informací musíme podepsat NDA dokument. Tento není součástí zadávací dokumentace. Chápeme toto rozlišení správně a je případně možné NDA podepsat?
2. Jaký je počet využívaných virtuálních serverů (tento údaj bychom potřebovali z důvodů případného licencování)?
3. V „Příloze 1- Technická specifikace předmětu zakázky“ jsou rozporuplné požadavky na množství EPS (konkrétně řádky bod 10, 12 a 15 tabulky).
    - V bodě 10 je zmiňováno 1000EPS a požadavek na možné rozšíření na 5000EPS. Vnímáme toto správně, že se jedná o rozšíření licence v případě budoucí potřeby navýšení (dlouhodobě se překračuje průměrně 1000EPS)?
    - V bodě 12 jsou uvedeny krátkodobé špičky až 7500EPS v délce 24hodin. Chápeme správně, že se jedná o stav, který může nastat v období 24 hodin například jednou nebo dvakrát a třeba na dobu 1minuty nebo je to kontinuální přísun logů po dobu 24 hodin?

4. V „Příloze 1- Technická specifikace předmětu zakázky“ v tabulce v bodě 1 je požadováno: „**Řešení musí být funkčně i technicky odděleno od ostatních částí systému“.** Jak toto máme chápat? Ukládání logů je nedílnou součástí SIEM řešení a úzce spolupracuje se SIEMem.
5. Je preferovaná varianta vlastních virtuálních serverů nebo dodání „fyzického železa“?
6. V „Příloze 1- Technická specifikace předmětu zakázky“ v tabulce v bodě 4 – je požadavek na retenci až na 13 měsíců, ZoKB hovoří o 18 měsících. Máme počítat s retencí 13 nebo 18 měsíců?
7. Existuje odhad velikosti logů, které budou za den vygenerovány?
8. Jaká je předpokládaná kapacit FPS (flows per second) v rámci síťové bezpečnosti?
9. V rámci zadávací dokumentace se hovoří o auditech kybernetické bezpečnosti. V „Příloze 1- Technická specifikace předmětu zakázky“ v bodě „2. Audit kybernetické bezpečnosti“ jsou zmiňovány penetrační testy. Máme chápat, že z pohledu Zadavatele je bezpečnostní audit = penetrační testování?
10. V „Příloze 1- Technická specifikace předmětu zakázky“ zřejmě nesouhlasí číslování oblastí. V úvodu na straně 2 je **bod 3. uveden jako „Služby poradenství a podpory“** níže v dokumentu konkrétně na straně 18 je již tento titulek pod **bodem 2 a s jiným názvem „Služby poradenství a podpor, resp. „Služby spojené s implementací IS“** – co je myšleno pod zkratkou IS?
11. V „podpůrných aktivech“ je uveden Vulnerability management systém – jaká je úloha SOCu u této oblasti (SOC vyhodnocuje výsledný sken nebo jaká je představa)?
12. V „Příloze 1- Technická specifikace předmětu zakázky“ je u modulu NetFlow sonda požadovaná instalace do 19racku s maximální velikostí 1U. Je přípustná velikost 2U (pro kapacitu 10Gps)?

Odpověď zadavatele:

Ad 1)
Ano pro větší podrobnosti je nutné podepsat NDA. V případě zájmu o informace označené NDA zašleme NDA.

Ad 2)
Počet serverů je cca 150.

Ad 3)
Aktuální průměrná hodnota EPS je cca 600. Pro případ rozšíření je právě uvedena hodnota 5000 EPS. Hodnota 7500 EPS je myšlena pouze jako krátkodobá za 24 hodin po dobu řádově minut.

Ad 4)
Tato část je myšlena tak, že systém pracuje samostatně, pouze sbírá logy a následně provádí jejich vyhodnocení. Není součástí např. emailového serveru.

Ad 5)
Není preferována ani jedna varianta.

Ad 6)
Krajský úřad Středočeského kraje provozuje pouze významné informační systémy dle Zákona č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), dle §3, písmena e. Tj. požadujeme retenci 13 měsíců.

Ad 7)
Průměrná velikost ukládaných logů je 60 GB/den.

Ad 8)
FPS – 150 průměrná hodnota

Ad 9)
Ano, jsou myšleny penetrační testy.

Ad 10)
Zkratkou IS myšleno Informační systém.

Ad 11)
Úloha SOCu je myšlena, že bude upozorňovat na zranitelnosti dohledovaných informačních systémů v rámci pravidelného reportingu zadavateli.

Ad 12)
Ano je přípustná velikost 2U.

V Praze dne 24. 7. 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: 2024.07.24 14:32:34 +02'00'