Vysvětlení zadávací dokumentace č. 3

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 1. 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:

K Příloze č. 1 – Technická specifikace předmětu zakázky:

1. Rozumíme správně, že předmětem služeb celku č. 2 jsou výhradně vyjmenované služby penetračního testování (testování vybrané webové aplikace, penetrační testování perimetru a penetrační testování vnitřního systému), a nikoliv jiné služby auditu kybernetické bezpečnosti, jak jsou popsány v §16 Vyhlášky (např. posouzení dodržování bezpečnostních politik a podobně)?

2. Jaká jsou podrobnější očekávání a rozsahy penetračního testování? Prosíme o podrobnější kvantifikaci cílových systémů - webových aplikací, perimetru i vnitřní infrastruktury.

3. Předimplementační analýza, referencovaná na str.2 v bodě 3.1 zejména vypracováni detailního popisu stávajícího stavu se má týkat výlučně aspektů uvedených v paragrafech 16, 17, 18, 22, 23, 24 a 27 Vyhlášky, a nikoliv jiných oblastí kybernetické bezpečnosti, uvedených např. v paragrafech 19, 20 a 21? Jaké podklady ohledem současného stavu, co do formy a rozsahu, bude zadavatel schopen poskytnout úspěšnému uchazeči?

4. V části “1.1. Zaznamenávání a ukládání logů a detekce bezpečnostních událostí” v tabulce v bodě 5 je uvedeno: "Řešení musí poskytnout vysokou dostupnost sběru logů (sběračů)." Můžete prosím lépe definovat, co je myšleno "vysokou dostupností"? Například dostupnost služby sběru logů větší než XY%? Nebo očekává zadavatel nějaké konkrétní vlastnosti HW a SW řešení proti výpadkům?

5. V části “1.1. Zaznamenávání a ukládání logů a detekce bezpečnostních událostí” v tabulce v bodě 20 je uvedeno: "Řešení Služby bude poskytovat automaticky backup/recovery procesu." Můžete prosím detailněji vysvětlit, co je myšleno tímto požadavkem?

6. V části “1.1. Zaznamenávání a ukládání logů a detekce bezpečnostních událostí” v tabulce v bodě 23 je uvedeno: "Systém musí umožňovat definici vlastního parseru pro jednotlivé zdroje logů a tím, že uživatelská konfigurace vlastních parserů pomocí vizuálního programovacího jazyka." Prosíme o upřesnění, co je myšleno pojmem "vizuální programovací jazyk"?

7. V části “1.1. Zaznamenávání a ukládání logů a detekce bezpečnostních událostí” v bodě 36 je uvedeno: "Požadujeme schopnost samostatného 'učení' normálního stavu. Podle nastavené bezpečnostní politiky pak reagovat na vznik skupinových nebo kontextuálních anomálií." Správně rozumíme, že zadavatel požaduje, aby součástí dodávaného řešení byla funkcionalita strojového učení a následné využití pro detekci anomálií? Pokud ano, na kterých ze zpracovávaných dat resp. typech událostí očekává zadavatel takovýto typ učení a detekce?

8. V části “1.1. Zaznamenávání a ukládání logů a detekce bezpečnostních událostí” v bodě 46 je uvedeno: "Řešení musí být navázáno na národní centrum kybernetické bezpečnosti CSIRT a publikovat v konzoli jím aktuálně uveřejněné hrozby." Prosíme o upřesnění, co je požadováno pod "navázáním” řešení na národní centrum kybernetické bezpečnosti?

9. V části “1.1. Zaznamenávání a ukládání logů a detekce bezpečnostních událostí” v bodě 47 je uvedeno: "SIEM použitý v řešení musí být zařazen do 5 posledních studií agentury Gartner (tzv. magických kvadrantů)." Správně předpokládáme, že zadavatel má na mysli publikace s názvem "Gartner Magic Quadrant for Security Information and Event Management"? Pokud ano, vzhledem k tomu, že se jedná o komerční materiály, jejichž získání je možné pouze pro klienty společnosti Gartner, prosíme buď o dodání těchto 5 referencovaných studií, nebo o upřesnění, případně vynechání tohoto požadavku.

10. V části “1.3. Zaznamenávání a ukládání logů a detekce bezpečnostních událostí” v bodě 2 je uvedeno: "Poskytovatel musí uvést adresu, kde jsou ukládána data SOC k prokázání zpracování dat v působnosti právních norem ČR." Vzhledem k tomu, že požadavky zadavatele směřují k řešení, kde data zadavatele jsou sbírána, vyhodnocována a ukládána na systémech instalovaných v jeho IT prostředí - ukládání jakých "dat SOC" je v této otázce myšleno?

11. V části “1.3. Zaznamenávání a ukládání logů a detekce bezpečnostních událostí” v bodě 16 je uvedeno: "Helpdeskový systém s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení." Správně předpokládáme, že helpdeskový systém s online přístupem zmíněný v tomto bodě je myšlen jako ITSM/ticketing systém provozovaný dodavatelem, který je přístupný bezpečným způsobem i pro pracovníky zadavatele?

Odpověď zadavatele:

Ad 1)
Ano, zadavatel předpokládá provedení penetračních testů.

Ad 2)
Zadavatel předpokládá testování vnějšího perimetru cca 50 vnějších IP adres. Testování webových aplikací, především související s provozovanými VIS (GINIS, spisová služba, portál krizového řízení, a dalších vybraných webových aplikací do počtu cca 30 ks). Dále testování vnitřní infrastruktury ve vybraném rozsahu. Zadavatel předpokládá provedení celkem 5 penetračních testů vybraných systémů v průběhu kontraktu 60 měsíců.

Ad 3)
Ano, předpokládá se pouze popisu v uvedených paragrafech. Zadavatel má k dispozici kompletní přehled a popis aktuálně napojených systémů do služby SOC.

Ad 4)
Předpokládá se dostupnost služby sběru logů větší než 95 %. Zadavatel neočekává konkrétní HW nebo SW vlastnosti.

Ad 5)
Zadavatel přepokládá automatické zálohování ukládaných logů.

Ad 6)
Zadavatel předpokládá definici vlastních parserů mimo "běžných" parserů používaných Poskytovatelem. Zadavatel poskytne požadavek na vlastní parser pomocí vizuální/grafické informace bez nutnosti znát programovací jazyk parserů Poskytovatele.

Ad 7)
Ano, předpokládá se především učení a detekce na síťovém provozu.

Ad 8)
Zadavatel předpokládá sledování aktuálních zveřejněných hrozeb ze strany Poskytovatele národním centrem kybernetické bezpečnosti CSIRT a informování Zadavatele o těchto hrozbách.

Ad 9)
Zadavatel tímto bez náhrady vypouští požadavek uvedený v příloze č. 1 zadávací dokumentace, podle čl. 1.1. Zaznamenávání a ukládání logů a detekce bezpečnostních událostí" v bodě 47, podle kterého měl být SIEM použitý v řešení zařazen do 5 posledních studií agentury Gartner (tzv. magických kvadrantů). Zadavatel tímto mění přílohu č. 1 zadávací dokumentace - Technická specifikace předmětu zakázky a coby přílohu k tomuto vysvětlení zadávací dokumentace předkládá revidovanou verzi Technické specifikace předmětu zakázky, která nahrazuje přechozí uveřejněné verze.

Ad 10)
Zadavatelem je myšleno zpracování a ukládání logů Zadavatele v rámci služby SOC Poskytovatele. Proto je nutné znát adresu ukládání a zpracování dat na straně Poskytovatele pro naplnění legislativních požadavků.

Ad 11)
Ano. Dodavatel správně předpokládá, že jde o ITSM/ticketing systém provozovaný dodavatelem, který je přístupný bezpečným způsobem i pro pracovníky zadavatele.

Zadavatel s ohledem na úpravy zadávacích podmínek současně v souladu s ust. § 99 odst. 2 zákona přiměřeně prodlužuje lhůtu pro podání nabídek do 28. 8. 2024 do 10:00 hodin.

Přílohy:

Příloha č. 1 - Technická specifikace předmětu zakázky – revize 2

V Praze dne 5. 8. 2024

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