FRÝDEK≈MÍSTEK

Statutární město Frýdek-Místek
Magistrát města Frýdku-Místku
Radniční 1148, 738 01 Frýdek-Místek

Odbor zadávání veřejných zakázek
pracoviště Radniční 1148, Frýdek

Váš dopis značka:
Ze dne:
Číslo jednací: MMFM 175381/2023
Spisová značka: 91.1
Vyřizuje: Bc. Ivo SZTWIERTNIA
Telefon: 558609292
E-mail: sztwiertnia.ivo@frydekmistek.cz
Datum: 11.10.2023

VYSVĚTLENÍ ZADÁVACÍCH PODMÍNEK

Veřejná zakázka: **Zajištění služby kybernetického bezpečnostního dohledu**
Evidenční číslo: P23V00000096
Druh veřejné zakázky: služby

Dotaz č. 1:
Zadavatel má právo a současně povinnost se v co nejvyšší možné míře snažit zabezpečit IT aktiva města. V odpovědi na otázku č. 2 zadavatel píše, že není podmínkou, aby dodavatel zajistil fungování služby bez potřeby spojení s externí službou v cloudu, přičemž kdyby zadavatel na takové podmínce trval, tak by odstranil rizika výpadku služby na transportní vrstvě, výpadku služby 3. strany v cloudu, rizika při zajištění důvěrnosti a integrity odpovědi.
Proč zadavatel nesleduje oprávněný zájem snižovat možné rizika v co nejvyšší možné míře?

Odpověď zadavatele:
Zadavatel vyhodnotil takové riziko jako minimální a přípustné.

Dotaz č. 2:
V odpovědi č. 5 zadavatele se píše " Zadavatel nevyžaduje přístup k logům, ty musí mít k dispozici poskytovatel, který je za provoz odpovědný. ..." V případě kybernetického útoku na město Olomouc v roce 2021, došlo ke kompletnímu ochromení IT infrastruktury města do té míry, že město Olomouc nebylo po určitou dobu schopno komunikovat na síťové úrovni a nebylo schopné se dostat k bezpečnostním logům a zjistit vektor útoku, a následně na základě těchto zjištění zvolit správný postup pro mitigaci dopadů tohoto útoku a disaster recovery postup. V případě podobného útoku by se město Frýdek Místek mohlo dostat do stejné situace. Naopak v případě lokálního přístupu k logům by se toto riziko minimalizovalo v porovnání s potřebou zjištění těchto informací výhradně ze zdrojů nacházejících se mimo jeho síť.
Proč zadavatel nesleduje opravněný zájem minimalizace rizik a nepožaduje kromě měsíčního reportu o výsledcích resp. lozích taky možnost lokálního přístupu k bezpečnostním logům?

Odpověď zadavatele:
Tuto situaci vnímáme přesně opačně, kdy může dojít ke kompromitaci lokálních zařízení a pro ty případy má potřebné logy poskytovatel služby, kterého je schopen zadavatel kontaktovat funkčním kanálem (např. telefonicky) a logy ze strany poskytovatele mohou být poskytnuty

okamžitě. Zadavatel navíc disponuje dedikovaným logovacím zařízením, kde se ukládají veškeré potřebné logy mimo službu kybernetického bezpečnostního dohledu.

Dotaz č. 3:
V otázce č.16 zadavatel nepožaduje aby " u řešení pro zajištění kompletního přehledu o DNS provozu z koncových stanic uživateli, aby byla oficiální dokumentace výrobce k dodanému řešení lokalizována do českého jazyka?"
Nabídka je předložena v úředním jazyce, kterým je v Česke republice jazyk český. Součástí teto nábidky je taky podrobný technický popis technologií pomocí kterých poskytovatel naplňuje technické požadavky zadavatele na požadovanou službu. To znamená, že oficiální technická dokumentace výrobců technologií pomocí, kterých poskytovatel bude naplňovať technické požadavky zadavatele musí být poskytnuta k dispozici v českém jazyce, aby bylo možno vyhodnotit či služba, kterou poskytovatel nabízí, taky skutečně a prokazatelně naplňuje technické požadavky zadavatele.
Proč tedy zadavatel nepožaduje oficiální technickou dokumentaci výrobce v českém jazyce?

Odpověď zadavatele:
Zadavatel požaduje podrobné technické dokumentace po poskytovateli služby v min. rozsahu definovaném v technické specifikaci, vztahující se k nabízené službě a tu požaduje zadavatel v českém jazyce. Zadavatel nepožaduje oficiální technickou dokumentaci výrobců technologií, pomocí kterých poskytovatel nabízenou službu hodlá zajistit. Z tohoto důvodu nepožadujeme, aby byla oficiální technická dokumentace jednotlivých technologií v českém jazyce, protože ji nepožadujeme vůbec.

Dotaz č. 4:
V dokumentu "1.specifikace predmetu plnění aktualizovano" v bodu 2.3 požaduje zadavatel "vypracovní a dodání podrobné technické dokumentace podle skutečného nasazení pro zaměstnance odboru IT objednatele v elektronické podobě", který je dle zákona třeba dodat v úředním jazyce.
Proč zadavatel vylučuje, aby oficiální technická dokumentace výrobce byla v českém jazyce, když požaduje vypracování a dodání podrobné technické dokumentace,
kterou je dle zákona nutno dodat v úředním jazyce?

Odpověď zadavatele:
Viz. odpověď v bodě 3., kdy zadavatel nepožaduje oficiální technickou dokumentaci k jednotlivým technologiím, pomocí kterých poskytovatel nabízenou službu hodlá zajistit. Zadavatel v technické specifikaci požadoval pouze VYPRACOVÁNÍ podrobné technické dokumentace podle skutečného nasazení nabízené služby, což vylučuje prosté zkopírování nebo předání oficiální technické dokumentace výrobce technologií, které budou pro zajištění služby poskytovatelem využity.
Zadavatel nepožaduje oficiální technickou dokumentaci výrobce, proto ani nemůže vylučovat, aby oficiální technická dokumentace výrobce byla v českém jazyce. Pokud poskytovatel předá oficiální technickou dokumentaci výrobce využívaných technologií, je to nad rámec požadavků dle technické specifikace.

Dotaz č. 5:
V dokumentu vysvětlení v otázce č. 2 se píše, že zadavatel požaduje "zajištění blokace bez potřeby spojení není podmínkou" a současně v odpovědi č. 6 píše, že " Ne- zadavatel nestanovuje, zda bude služba zabezpečení DNS provozu zajištěna nástroji lokálně nebo v cloudu" a současně v odpovědi č.9. nepožaduje "u řešení pro zajištění kompletního přehledu o DNS provozu z koncových stanic uživateli zajištění rekurzivního překladu DNS požadavku" a taky v odpovědi č. 7 "zadavatel nepřipouští u zabezpečení DNS provozu instalace SW popř. agentů na koncových stanicích. Zadavatel připouští změnu konfigurace koncových stanic např. hromadnými politikami GPO nebo v rámci DHCP request-response komunikace.".
Pro DNS security je nezbytné, aby blokace byla zajištěna bez potřeby spojení se službou v cloudu nebo je potřeba vykonávat tuto blokaci pomocí instalace SW / agentu na koncových stanicích, které současně zabezpečí rekurzivní překlad DNS požadavku. Odpovědi zadavatele vzájemně

vylučují, aby požadovaná služba poskytovala blokování nelegitimních DNS dotazů, ale dle odpovědí zadavatele se jedná jen o cloudovou verzi Proxy serveru.
Požaduje zadavatel službu cloudové verze Proxy serveru, která hlídá a blokuje nelegitimní dotazy nebo požaduje zadavatel zabezpečení DNS formou hlídání a blokaci nelegitimních DNS dotazů a tedy požaduje, že blokace bude zajištěna bez potřeby spojení se službou 3. strany v cloudu, resp. připouští instalaci SW/agenta pro zabezpečení DNS provozu se zajištěním rekurzivního překladu DNS požadavku.

Odpověď zadavatele:
z uvedeného komentáře nelze vyčíst dotaz. Zadavatel požaduje pouze kontrolu DNS dotazů, kdy následný překlad bude řešit interní DNS server zadavatele (v případě interních dotazů) a DNS server na Ministerstvu vnitra v rámci uzavřené sítě CMS2, který pro zadavatele dělá překlad veškerých dotazů kromě interních (směřujících do internetu). Zadavatel upřesnění zaznamenal do přílohy Specifikace předmětu plnění.

Dotaz č. 6:
V odpovědi č.12 zadavatel požaduje "při službě na blokaci závadných adres DNS také funkci, aby blokace směřovala na blokační stránku, kterou lze upravit dle vizuální identity veřejného zadavatele (např. fonty, barvy logo města, kontaktní údaje)."
V případě zabezpečení funkce blokační stránky výhradně v cloudu, vzniká riziko kompromitace takové odpovědi nebo výpadku této služby.
Požaduje zadavatel eliminaci tohoto rizika při službě na blokaci závadných DNS adres pomocí technologie, která poskytuje funkci blokační stránky jak lokálně, tak v cloudu nebo jen pomocí funkce blokační stránky poskytované lokálně?

Odpověď zadavatele:
Způsobem blokace se rozumí přesměrování na interní blokační informační stránku.

Dotaz č. 7:
Chápeme správně, že při hlídání a blokaci nelegitimních DNS dotazů, se také požaduje hlídání a blokace DNS dotazů souvisejících s bezpečnostními incidenty jako jsou:
a) nelegitimní DNS tunneling,
b) nelegitimní DNS tunneling legitimních poskytovatelů služeb jako jsou Microsoft, Oracle apod. u kterých existuje důvodné podezření z exfiltrací dat,
c) blokování nelegitimních DNS dotazů na nelegitimní destinace definované legislativou ČR,
d) cílený phishingový útok (targeted phishing attack, spear-phishing),
e) man in the middle útok,
f) hlídaní a blokaci nelegitimních DNS dotazů pomocí DNSSEC validace zahrnující NSEC3 podporu nebo negativní cashing.

Odpověď zadavatele:
Ne, toto zadavatel nepožaduje.

Zadavatel uveřejnil na profilu zadavatele aktualizovanou přílohu **Specifikace předmětu plnění.**

Zadavatel prodlužuje lhůtu pro podání nabídek do 16. 10. 2023 do 9:00 hodin.

Mgr. Roman Šebesta
vedoucí odboru zadávání veřejných zakázek