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 166972/2023
Spisová značka: 91.1
Vyřizuje: Bc. Ivo SZTWIERTNIA
Telefon: 558609292
E-mail: sztwiertnia.ivo@frydekmistek.cz
Datum: 27.09.2023

VYSVĚTLENÍ ZADÁVACÍCH PODMÍNEK

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

Zadavatel v rámci výše uvedeného zadávacího řízení obdržel dodatečné dotazy následujícího znění:

1. Kolik koncových stanic uživatelů/virtuálních serveru má být pod kontrolou systému pro monitoring a zabezpečení DNS provozu?

   Odpověď zadavatele: *550 koncových stanic 110 serverů.*

2. Požaduje zadavatel, aby dodané řešení pro zabezpečení DNS provozu zajišťovalo blokaci závadných adres bez potřeby spojení se službou v cloudu (a to zejména ale ne výhradně z důvodů eliminace rizika výpadku služby na transportní vrstvě, eliminaci rizika výpadku služby 3. strany v cloudu, z důvodu zajištění důvěrnosti a integrity odpovědi)?

   Odpověď zadavatele: *Zajišťování blokace bez potřeby spojení není podmínkou.*

3. Požaduje veřejný zadavatel, aby poskytovatel služby kybernetického bezpečnostního dohledu poskytoval pomocí již existujících technologií na straně veřejného zadavatele, resp. dodaných technologií pro poskytnutí pořizované služby, také informaci o únicích identit zaměstnanců městského úřadu a automatizované alertování takových bezpečnostních incidentů, pokud by k úniku identit zaměstnance městského úřadu došlo v budoucnosti?

   Odpověď zadavatele: *Požadujeme, aby poskytovaná služba byla realizována technologií dodanou poskytovatelem. Ano, požadujeme informace o únicích identit zaměstnanců zadavatele (viz bod 2.2 technické specifikace). Co se týče poskytování těchto informací v rámci služby, zadavatel požaduje, aby došlo k neprodlenému informování, zadavatel neřeší, jakým způsobem toto poskytovatel zajistí.*

4. Požaduje zadavatel zajištění zabezpečení DNS provozu z koncových stanic v oblasti kategorizace také pro blokaci závadných adres, které jsou požadovány regulátorem v ČR? (např.: Ministerstvo financí ČR, SUKL ČR, Státní zemědělská a potravinářská inspekce ČR, Státní veterinární správa ČR, NUKIB ČR, a další)?

   Odpověď zadavatele: *Ne.*

5. Požaduje zadavatel lokální přístup k logům bez potřeby využití služby v cloudu?

   Odpověď zadavatele: *Ne – zadavatel nestanovuje, zda bude služba zabezpečení DNS provozu zajištěna nástroji lokálně nebo v cloudu. Zadavatel nevyžaduje přístup k logům, ty musí mít k dispozici poskytovatel, který je za provoz odpovědný. Zadavatel požaduje, aby služba zabezpečení DNS provozu plnila funkci blokace a dalších specifikovaných, byla součástí dohledu poskytovatele, tak aby mohl o anomáliích zadavatele informovat. O výsledcích, popř. lozích bude poskytovatel informovat v rámci měsíčního reportu.*

6. Požaduje zadavatel při řešení na zabezpečení DNS provozu s blokací závadných adres, aby bezpečnostní logy o blokovaných incidentech neopustily interní síť zadavatele, tedy byly zasílány z řešení pro zabezpečení DNS provozu s blokací závadných adres přímo do SIEM nástroje? A to zejména ale ne výhradně z důvodu zajištění důvěrnosti a integrity logů, z důvodů eliminace rizika výpadku služby na transportní vrstvě, eliminace rizika výpadku služby 3 strany v cloudu?

   Odpověď zadavatele: *Ne – zadavatel nestanovuje, zda bude služba zabezpečení DNS provozu zajištěna nástroji lokálně nebo v cloudu.*

7. Požaduje zadavatel při řešení na zabezpečení DNS provozu s blokací závadných adres koncových stanic uživateli, aby řešení nevyžadovalo modifikaci na koncových stanicích, tedy má být bez potřeby instalace SW na koncové stanici, jakož i bez potřeby instalace certifikátů nebo přenastavení bezpečnostních politik?

   Odpověď zadavatele: *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.*

8. Požaduje zadavatel zabezpečení DNS provozu s blokací závadných adres koncových stanic uživateli poskytovalo funkci dostupnosti DNS traffic logu v jednotném rozhraní s možností exportu v .csv. formátu?

   Odpověď zadavatele: *Ne zadavatel toto nepožaduje, nicméně může si od poskytovatele vyžádat log DNS trafficu po poskytovateli ve standartně čitelném formátu.*

9. Požaduje zadavatel u řešení pro zajištění kompletního přehledu o DNS provozu z koncových stanic uživateli zajištění rekurzivního překladu DNS požadavku?

   Odpověď zadavatele: *Ne.*

10. Požaduje zadavatel z důvodu, že při blokaci závadných adres DNS službou se jedná současně o byznys kritickou službu, aby rekonfiguraci a také aktualizaci, update a upgrade takového řešení bylo možné provést za plného provozu, bez potřeby downtime služby a bez DNS traffic výpadku?

    Odpověď zadavatele: *Ne – poskytovatel bude provádět aktualizace a rekonfigurace mimo pracovní dobu zadavatele po předchozí domluvě s IT.*

11. Požaduje zadavatel při blokaci závadných adres DNS službou při blokaci také funkci bypass pro celé segmenty sítě?

Odpověď zadavatele: *Ne.*

12. Požaduje zadavatel při službě na blokaci závadných adres DNS také funkci aby blokace směřovala na blokační stránku, kterou lze upravit podle vizuální indentity veřejného zadavatele (např. fonty, barvy logo města, kontaktní údaje)?

    Odpověď zadavatele: *Ano.*

13. Požaduje zadavatel u řešení pro zajištění kompletního přehledu o DNS provozu z koncových stanic uživateli z důvodů zabezpečení disaster recovery managementu tohoto řešení možnost konfigurace taky přímo z příkazové řádky?

    Odpověď zadavatele: *Ne – zadavatel nestanovuje pomocí jakého rozhraní bude poskytovatel službu konfigurovat.*

14. Požaduje zadavatel u řešení pro zajištění kompletního přehledu o DNS provozu z koncových stanic uživateli, aby byla řídící konzole lokalizována do českého jazyka?

    Odpověď zadavatele: *Ne.*

15. Požaduje zadavatel u řešení pro zajištění kompletního přehledu o DNS provozu z koncových stanic uživateli podporu pro 3. level (nejvyšší) podpory přímo od výrobce technologie v českém jazyce?

    Odpověď zadavatele: *Ne – zadavatel nestanovuje úroveň podpory, jelikož je za bezchybný provoz služby odpovědný poskytovatel.*

16. Požaduje zadavatel 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?

    Odpověď zadavatele: *Ne.*

17. Chápeme správně, že zadavatel chce, aby SIEM byl provozován přímo u něj a operátoři SOC se k němu připojovali? Pokud ano, tak si dovolíme upozornit, že tato varianta je zásadně nákladnější než využití SIEM v rámci dohledového centra žadatele.

    Připouští zadavatel variantně umístit na jeho straně kolektor, který bude logy přeposílat k žadateli? Pokud nikoliv dovolujeme si upozornit, že kvalitní implementace SIEM nástroje včetně kontentu se pohybuje mezi 6 až 10 měsíci.

    Odpověď zadavatele: *Ano, zadavatel připouští kolektor na své straně, kdy logy budou přeposílány poskytovateli.*

18. Zadavatel uvádí, že požaduje zajištění zabezpečení DNS provozu koncových stanic *uživatelů* blokací závadných adres s možností kategorizace a zajištění kompletního přehledu o DNS provozu z koncových stanic uživatelů v reálném čase. Má zadavatel již stávající technologii, kterou chce napojit do SIEM, nebo zadavatel požaduje dodat?

    Odpověď zadavatele: *Ne, zadavatel nedisponuje takovou technologií, ta musí být součástí služby.*

19. Zadavatel uvádí, že požaduje vykonávání kybernetického bezpečnostního dohledu v režimu 24x7x365, kdy operátor musí být i v tomto režimu na svém pracovišti (forma pohotovosti není přípustná a objednatel toto může kdykoliv libovolně kontrolovat), zahájení řešení bezpečnostního incidentu, možnost kontaktu poskytovatele objednatelem s žádostí o řešení problému spojeného s poskytovanou službou, s žádostí o konzultaci.

    Prosíme o informaci, zda zadavatel funguje v režimu 24x7x365 a bude schopen na případné tickety, nebo telefonáty ze strany SOC reagovat? Jedná se o cenově náročný model SLA a v případě, že by zadavatel tento režim neměl zavedený, tak se jedná o

neekonomické řešení. Je zadavatel ochoten připustit model, kdy mimo pracovní dobu je režim SOC v pohotovostním módu?

Odpověď zadavatele: *Zadavatel požaduje režim 24x7.*

20. Zadavatel uvádí, že jednou za dva měsíce musí poskytovatel provést sken zranitelností v interní infrastruktuře objednatele, nebo na vyžádání, a to v režimu 24x7x365 (se spuštěním skenu do 1 hod.).

    Má zadavatel nějaký konkrétní nástroj k dispozici nebo požaduje jeho dodání?

    Odpověď zadavatele: *Ne, zadavatel nedisponuje takovým nástrojem, ten musí být součástí dodávky.*

21. Zadavatel uvádí, neprodleně poskytovat informace o únicích informací a dat o doméně a uživatelích objednatele na Dark webu.

    Má zadavatel k dispozici nástroj a set informací, které se mají na Dark webu prohledávat, nebo si přeje nástroj dodat?

    Odpověď zadavatele: *Ne, zadavatel nedisponuje takovým nástrojem, ten musí být součástí dodávky.*

Zadavatel prodlužuje lhůtu pro podání nabídek do 11. 10. 2023 do 9:00 hodin.

Mgr. Roman Šebesta
vedoucí odboru zadávání veřejných zakázek