Číslo spisu: NBS1-000-106-411
Číslo záznamu: 100-000-890-440
Dátum: 24.4.2025

VYSVETLENIE

informácií potrebných na vypracovanie ponuky a na preukázanie splnenia podmienok účasti podľa § 48 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „ZVO“)

Národná banka Slovenska so sídlom Imricha Karvaša 1, 813 25 Bratislava (ďalej len „verejný obstarávateľ“) obdržala prostredníctvom elektronického prostriedku, komunikačného rozhrania systému JOSEPHINE žiadosti o vysvetlenie podľa § 48 ZVO týkajúce sa predmetnej zákazky.
Po podrobnom oboznámení sa so žiadosťami o vysvetlenie Vám verejný obstarávateľ poskytuje nasledujúce vysvetlenie:

Otázka č. 18:
V prílohe č.7 Zoznam špecifických use caseov.docx, sú jednotlivé use case vymenované. - detekcia zneužívania komunikačných kanálov malware na SWIFT serveroch Mohli by sme požiadať o spresnenie toho use-case v zmysle, či systém alebo externý nástroj detekuje priamo pokusy o zneužitím, alebo či ide napríklad o detekciu na základe indikátorov, ktoré sú dodávané bankou?

Odpoveď:
Verejný obstarávateľ spresňuje špecifický use case - detekcia zneužívania komunikačných kanálov malware na SWIFT serveroch. V tomto prípade sa jedná o detekciu pokusov využívania lokálnych SWIFT komunikačných kanálov inými aplikáciami ako SWIFT. Detaily o jednotlivých use casoch budú poskytnuté úspešnému uchádzačovi.

Otázka 19:
V prílohe č.7 Zoznam špecifických use caseov.docx, sú jednotlivé use case vymenované. - integrácia udalostí zo SWIFT V akom zmysle bude implementovaný use-case? Ide o zobrazenie udalostí, ktoré systém generuje 1:1 v rámci SIEM priamo zo SWIFT?

Odpoveď:
Verejný obstarávateľ spresňuje špecifický use case - integrácia udalostí zo SWIFT. V tomto prípade sa jedná o preposielanie udalostí zo SWIFT aplikácií a SWIFT Gateways do SIEMu, ich normalizáciu do jednotného formátu a následné spracovanie v SIEMe. Detaily o jednotlivých use casoch budú poskytnuté úspešnému uchádzačovi.

Otázka č. 20:
Verejný obstarávateľ v bode 6. Čl. X Zmluvy upravuje mechanizmus nahradenia dodávateľa iným dodávateľom podľa § 18 zákona č. 343/2015 Z. z. o verejnom obstarávaní, v prípade podstatného porušenia Zmluvy poskytovateľom, pričom zo zmluvných ustanovení v Čl. IX bode 1 vyplýva, že za podstatné porušenie Zmluvy sa považuje akékoľvek neposkytnutie plnenia podľa Prílohy č.1 Zmluvy a to bez zohľadnenia závažnosti samotného porušenia.

Na základe uvedeného vyššie Verejný obstarávateľ môže vykonať zmenu dodávateľa iným dodávateľom aj v prípade, ak bude napr. pri Službe MBIT táto služba jednorazovo poskytnutá v inom ako požadovanom časovom okne, pričom sa nemusí jednať o nijako zásadné a ani opakované porušenie poskytovaných služieb s dopadom na celkovú úroveň zabezpečenia kybernetickej a informačnej bezpečnosti organizácie.
Máme za to, že takto nastavené podmienky Zmluvy sú nevyvážené a neproporcionálne vzhľadom k plneniu, ktoré sa požaduje zabezpečiť. Z uvedeného dôvodu žiadame Verejného obstarávateľa, aby zmenil definíciu podstatného porušenia Zmluvy len vo vzťahu k takým Službám, ktoré sú vzhľadom na svoj charakter a prevádzkové podmienky organizácie skutočne kritické.

Odpoveď:
Verejný obstarávateľ vzhľadom na to, že prehodnotil prísnosť predmetného zmluvného ustanovenia tak, aby vytvoril predpoklady pre čo najširšiu hospodársku súťaž, upravuje bod 1 článku IX Zmluvy, pričom tento bod znie: „V prípade neposkytnutia predmetu plnenia v súlade so stanovenými požiadavkami, a to aj jednotlivou požiadavkou, na poskytované služby podľa Prílohy 1 Zmluvy, okrem Služby Monitoring bezpečnosti IT (SOC), Služby Monitoring a prevádzka MBIT (SIEM a NDR), Služby Rozvoj a optimalizácia MBIT a Služby ‚Forenzná analýza', je objednávateľ oprávnený požadovať od poskytovateľa zmluvnú pokutu vo výške 300 eur bez DPH, a to za každé jednotlivé porušenie záväzku, pričom v prípade neposkytnutia Služby Monitoring bezpečnosti IT (SOC), Služby Monitoring a prevádzka MBIT (SIEM a NDR), Služby Rozvoj a optimalizácia MBIT alebo Služby ‚Forenzná analýza' v súlade so stanovenými požiadavkami, a to aj jednotlivou požiadavkou podľa Prílohy 1 Zmluvy je objednávateľ oprávnený požadovať od poskytovateľa zmluvnú pokutu vo výške 1000 eur bez DPH, a to za každé jednotlivé porušenie záväzku. Zároveň sa minimálne raz opakované porušenie záväzku poskytovať Službu Monitoring bezpečnosti IT (SOC), Službu Monitoring a prevádzka MBIT (SIEM a NDR), Službu Rozvoj a optimalizácia MBIT alebo Službu ‚Forenzná analýza' v minimálnych podmienkach (aj čo i len jednej podmienke) upravených v Prílohe 1 tejto Zmluvy považuje za podstatné porušenie Zmluvy.".

Otázka č. 21
Verejný obstarávateľ požaduje v rámci Implementačných prác a služieb, aby Poskytovateľ zabezpečil demontáž zariadení, ktoré budú nahradené novými zariadeniami a súčasne znášal náklady spojené s demontážou a odvozom ako aj odstránením pôvodnej konfigurácie zariadení. Verejný obstarávateľ však nikde v Súťažných podkladoch nešpecifikuje počet voľných pozícií v rozvádzačoch ako ani miesto odvozu demontovaných zariadení. Na základe uvedených informácií nie je zrejmé, či bude skutočne potrebné vykonať demontáž jestvujúcich zariadení, stanoviť jej rozsah vrátane prevozu na požadované miesto a teda určiť celkovú prácnosť požadovanej aktivity.
Žiadame Verejného obstarávateľa, aby v súlade s § 42 zákona č. 343/2015 Z. z. o verejnom obstarávaní jednoznačným spôsobom definoval, čo sa má v rámci implementačných prác a služieb v skutočnosti vykonať, alebo alternatívne aby Verejný obstarávateľ v zmysle uvedeného v rámci Všeobecných požiadaviek (bod 2.6 záložka „Všeobecné požiadavky") zabezpečil miesto v rozvádzačoch ako aj horeuvedené aktivity vo vlastnej réžií.
Odpoveď:
Verejný obstarávateľ uvádza, že požiadavka 3.7 sa týka demontáže a odvozu zariadení, ktoré si dodá do priestorov objednávateľa samotný poskytovateľ, aby poskytoval predmet plnenia

v rozsahu požiadaviek predmetu zákazky. Verejný obstarávateľ vysvetľuje požiadavku v bode 3.7. nasledovne: „Uchádzač zabezpečí demontáž ním dodaných zariadení po skončení trvania zmluvy. Náklady spojené s demontážou a odvozom zariadení bude preto prirodzene znášať poskytovateľ." Miesto odvozu demontovaných zariadení verejný obstarávateľ neustanovuje nakoľko sú majetkom/vlastníctvom poskytovateľa. Počet existujúcich zariadení a ich umiestnenie je uvedený v prílohe 10 SP (Základné informácie o IT prostredí NBS). Verejný obstarávateľ zabezpečí pre dodané zariadenia potrebné pozície v rozvádzačoch.

Otázka č. 22:
Verejný obstarávateľ v bode 4.2 Súťažných podkladov uvádza: „Cieľom predmetu zákazky „Monitoring kybernetickej bezpečnosti" je zabezpečenie kontinuity poskytovania služieb minimálne v súčasnej kvalite a rozsahu a ich rozšírenie o skenovanie zraniteľností a BAS služby."
Rozumieme tomu správne, že ostatné služby okrem skenovania zraniteľností a BAS ako napr. SIEM už sú v súčasnosti v prostredí Verejného obstarávateľa prevádzkované a budú v rámci tohto projektu plne nahradené v celom rozsahu Prílohy č.1 – Špecifikácie predmetu zákazky?

Odpoveď:
Verejný obstarávateľ spresňuje informáciu. V súčasnosti nie je prevádzkovaná iba BAS služba. Ostatné služby sú prevádzkované, vrátane skenera zraniteľnosti. Verejný obstarávateľ požaduje poskytovanie služieb uvedených v prílohe č.1 v plnom rozsahu.

Otázka č. 23:
Verejný obstarávateľ uvádza, že ponuky uchádzačov bude vyhodnocovať na základe ekonomicky najvýhodnejšej ponuky, použitím kritérií najnižšej ceny za predmet zákazky v kombinácii s kvalitatívnymi kritériami kvality expertného tímu dodávateľa. V bode 36.4 Verejný obstarávateľ uvádza, že kvalita tímu kľúčových osôb bude založená na osobných praktických skúsenostiach kľúčových osôb určených na plnenie zmluvy, pričom sa tím skladá z celkovo z 5 expertov pre celkovo 5 požadovaných rolí. Verejný obstarávateľ v bode 34.1.5 Súťažných podkladov uvádza, že pre splnenie podmienok účasti uchádzačov podľa § 34 ods. 1 písm. g) zákona č. 343/2015 Z. z. o verejnom obstarávaní požaduje rádovo 13 rôznych expertov na uvedených 5 rolí expertov.
Akým spôsobom bude Verejný obstarávateľ zohľadňovať aj skúsenosti ďalších expertov, ktorí tvoria tím expertov, nakoľko pre účely plnenia zo zmluvy ako aj splnenie podmienok účasti sa bude podieľať na jednej pozícií viacero expertov paralelne?

Odpoveď:
Verejnému obstarávateľovi postačuje splnenie minimálnej kvality premietnutej v podmienkach účasti pre každú osobu, ktorá bude plniť predmet zmluvy. Zároveň verejný obstarávateľ vytvára predpoklady aby získal skúsenejšieho experta do tímu pre každú z rolí. Zabezpečí sa tým to, aby poskytovateľov tím mal ku každej z piatich rolí aspoň jedného skúseného experta za ktorého je verejný obstarávateľ ochotný zaplatiť naviac.

Otázka č. 24
Aké konkrétne minimálne požiadavky na praktické skúsenosti pre jednotlivé role budú u jednotlivých expertov bodovo ohodnotené, a súčasne akým spôsobom bude Verejný

obstarávateľ pristupovať k hodnoteniu toho, či daná praktická skúsenosť úzko súvisí s predmetom zákazky alebo nie?

Odpoveď:
Verejný obstarávateľ si týmto dovoľuje uviesť, že minimálne požiadavky na honorovanú skúsenosť je upravená v bode 34.1.5.2 súťažných podkladov.

Otázka č. 25
Na základe akého predpokladu Verejný obstarávateľ očakáva, že kvantitatívne vyšší počet praktických skúseností experta zabezpečí vyššiu kvalitatívnu úroveň expertného tímu a teda aj poskytnutých služieb, na základe ktorých by bolo možné prideliť body v rámci vyhodnocovania ponúk?

Odpoveď:
Na základe dôvodného predpokladu. Existuje všeobecne akceptovaný predpoklad, že ak má niekto viac osobných praktických skúseností s činnosťou alebo podobnou činnosťou, ktorú má následne vykonávať, tak ju bude robiť lepšie, kvalitnejšie než niekto, kto má takých osobných praktických skúseností menej. Zároveň verejný obstarávateľ stanovil maximálny počet osobných praktických skúseností, ktoré bude honorovať z pohľadu marginálneho úžitku.

Otázka č. 26
Na základe akého dôvodu nebude Verejný obstarávateľ hodnotiť skúsenosti expertov, ktorými preukazuje uchádzač splnenie podmienok účasti, ak tieto osoby súčasne budú vykonávať jednotlivé role v prípade podpisu Zmluvy? V prípade, že tieto osoby nie je možné zahrnúť do hodnotenia kvality tímu, ich uvedenie v ponuke by malo vyslovene formálny charakter a súčasne by takýto spôsob vyhodnocovania ponúk nereflektoval skutočnú kvalitatívnu úroveň expertného tímu dodávateľa.

Odpoveď:
Verejnému obstarávateľovi postačuje splnenie minimálnej kvality premietnutej v podmienkach účasti pre každú osobu, ktorá bude plniť predmet zmluvy. Zároveň verejný obstarávateľ vytvára predpoklady preto aby získal skúsenejšieho experta do tímu pre každú z rolí. Zabezpečí sa tým to, aby poskytovateľov tím mal ku každej z piatich rolí aspoň jedného skúsenejšieho experta za ktorého je verejný obstarávateľ ochotný zaplatiť naviac.

Otázka č. 27:
V prílohe č.9 SP Opis predmetu zákazky - Požiadavky na predmet zákazky -
Verejný obstarávateľ v záložke s názvom “Sledovanie IT hrozieb a zraniteľností“ V bode 2.162 požaduje „Denné vyhodnocovanie aktuálnych IT hrozieb a zraniteľností z overených externých zdrojov“.
Požadujete aby súčasťou EASM bol aj monitoring hrozieb voči vašej spoločnosti/značke? Napr. phishingove kampane, Impersonacia, monitoring únikov dát, Domain Typosquatting a podobne? Má byť súčasťou služby aj OSINT, Intelligence Gathering z Darknet-u, sledovanie potenciálnych hrozieb v rámci Vášho dodávateľského kanálu, prípadne vyhľadávanie IoC v rôznych databázach?

Odpoveď:
Verejný obstarávateľ objasňuje účel služby "Sledovanie IT hrozieb a zraniteľností". Cieľom služby je sledovanie aktuálnych zraniteľností a hrozieb publikovaných na overených externých zdrojoch s cieľom identifikovať potenciálne bezpečnostné hrozby pre IT NBS. Služba má pokrývať sledovanie zraniteľností a hrozieb v technológiách NBS, ktoré nie sú zachytené skenerom zraniteľností napr. z dôvodu, že na daný systém nie je možné nainštalovať skenovacieho agenta, resp. využiť technologický účet.

Otázka č. 28:
V prílohe č.9 SP Opis predmetu zákazky - Požiadavky na predmet zákazky Verejný obstarávateľ v záložke s názvom " BAS" V bode 2.176 požaduje„ Prispôsobiť scenáre testovania napr. proti hrozbám zameraným na systémy SWIFT".
Otázka: V systéme, ktorý plánujeme použiť vieme prispôsobovať scenáre testovania vo forme špecifikovania payloadu, ktorý ma byť doručený/exekuovaný v rámci scenára. Payload je možné doručovať rôznym spôsobom, s využitím rozličných protokolov ako napr. HTTP, HTTPS, SMTP, a iné, pripadne ako custom PCAP replay. Je toto dostatočné prispôsobenie scenára? V prípade, ak nie prosím popíšte aké prispôsobenie scenárov požadujete.

Odpoveď:
Verejný obstarávateľ objasňuje požiadavku uvedenú v bode 2.176 „Prispôsobiť scenáre testovania napr. proti hrozbám zameraným na systémy SWIFT". Verejný obstarávateľ prispôsobením scenára má na mysli možnosť definovať vlastné techniky a taktiky, ktoré sú predmetom testovania tak, aby zodpovedali aktuálnym hrozbám pre cieľové prostredie.

Otázka č. 29:
V prílohe č. 9 SP Opis predmetu zákazky - Požiadavky na predmet zákazky Verejný obstarávateľ v záložke s názvom " BAS" V bode 2.183 požaduje „Integráciu s existujúcimi bezpečnostnými nástrojmi ako sú systémy SIEM, EDR a skener zraniteľnosti"
Otázka: Rozumieme integrácii s bezpečnostným systémom SIEM, ale nie je nám jasná požiadavka na integráciu so systémom EDR a skener zraniteľnosti. Môžete, prosím, popísať ako požadujete integrovať systém BAS so systémom EDR a skener zraniteľnosti?

Odpoveď:
Verejný obstarávateľ spresňuje informáciu. V prípade EDR a skenera zraniteľností ide o využitie informácií z týchto technológií pre účely BAS, ak toto ponúkané BAS riešenie poskytuje.

Otázka 30:
Príloha č. 9 SP Opis predmetu zákazky – Požiadavky na predmet zákazky
Zadanie - záložka v .xls "Všeobecné požiadavky", bod 2.10
SOC tím bude mať prístup do SD (riešenie žiadostí a incidentov) a podporných technológií NBS (Trellix ePO, Trellix ATD, Trellix EDR, Barracuda, WAF, Infoblox DNS, Fortinet a pod.) pre potreby prešetrovania bezpečnostných zistení v IT NBS.
Otázka:
V predmete zákazky nie je presne určená zodpovednosť a hranice prístupu k informáciám pre SOC tím dodávateľa. Má SOC tím zodpovednosti a povinnosti tieto nástroje aktívne využívať pri

došetrovaní udalostí alebo nie? Ak nie, potom informačná hodnota pre vyšetrovanie končí na strane SIEM-u ako zberu dát a ďalej už nepokračuje – napríklad by sa neprešetrovali bezpečnostné udalosti v EDR (z našej praxe je takmer vždy nevyhnutné ísť priamo do EDR na dôkladné prešetrenie, pretože nie všetky dáta má SIEM k dispozícii), ani by sa nedoťahovali podrobnejšie informácie z ďalších bezpečnostných riešení – Trellix, Sandbox, WAF, DDOS a pod. Teda rozhodovacie možnosti SOC tímu na strane dodávateľa by končili pri SIEM-e a ďalšie vyšetrovanie na konkrétnych bezpečnostných komponentoch by vykonávali vaši pracovníci, ktorí by sa tak aktívne zapájali do procesu riešenia bezpečnostných udalostí a boli by súčasťou riešiteľského tímu vrátane rozhodovania o type udalosti z bezpečnostného pohľadu. Išlo by teda o zdieľanú zodpovednosť medzi dodávateľom a objednávateľom pri riešení bezpečnostných incidentov. Je nevyhnutné toto presne špecifikovať a určiť, kam siaha rozsah dodávky ponúkaných služieb a zodpovedností.

Odpoveď:
Verejný obstarávateľ si Vám týmto dovoľuje uviesť, že požiadavky na SOC službu a z toho vyplývajúce zodpovednosti sú uvedené v bodoch 2.43 až 2.53 Opisu predmetu zákazky, Prílohy 9 SP. Verejný obstarávateľ požaduje aby SOC tím v plnom rozsahu vyšetril bezpečnostné zistenia. Na prípadné došetrenie zistení, tak ako je uvedené v bode 2.10 Opisu predmetu zákazky, Prílohy 9 SP, uchádzač bude mať k dispozícii prístup do podporných technológií. Takisto sa od uchádzača požaduje poskytnutie súčinnosti pri riešení bezpečnostných zistení až do ich úplného vyriešenia a odstránenia dôsledkov. Prípadný aktívny zásah je v kompetencii zamestnancov NBS. Primárne verejný obstarávateľ zabezpečuje prevádzku podporných technológií, nie vyšetrovanie bezpečnostných zistení.

Otázka 31:
Zadanie - záložka v .xls "MBIT (SIEM a NDR)", bod 2.130
Monitorované zariadenia a aplikácie logujú na logserver umiestnený v ich lokalite, t.j. HTP alebo ZTP. Logserver môže byť tvorený aj viacerými zariadeniami, pričom výpadok jedného zo zariadení zabezpečujúceho funkcionalitu logservera v danej lokalite nesmie znemožniť funkcionalitu samotného logservera.
Zadanie - záložka v .xls "MBIT (SIEM a NDR)", bod 2.131
V prípade úplného výpadku logservera v jednej lokalite, musí logserver v druhej lokalite prevziať funkcionalitu vypadnutého logservera a to tak, aby nebola potrebná rekonfigurácia agentov/zariadení zasielajúcich dáta do systému SIEM.
Otázka:
Prosíme o spresnenie a rozlíšenie požiadavky na funkcionalitu HA.
Pri vysokej dostupnosti rozlišujeme medzi HA pre:

- zber udalostí,
- spracovanie udalostí,
- ukladanie udalostí do databázy,
- prezeranie týchto udalostí a riešenie udalostí v rámci alertov a incidentov (cases).

Ktoré z daných funkcionalít majú byť dodané s vysokou dostupnosťou? A má byť táto dostupnosť zabezpečená aj naprieč lokalitami?

Odpoveď:

Verejný obstarávateľ si Vám týmto dovoľuje uviesť, že v uvedených v bodoch 2.130 a 2.131 Opisu predmetu zákazky, Prílohy 9 SP sú ciele požiadaviek také, aby v prípade rozpojenia HTP a ZTP alebo poruchy logservera v danej lokalite nedošlo k strate udalostí v dôsledku nemožnosti posielať udalosti do nedostupného logservera. Primárnym cieľom je kontinuálny zber udalostí. Ostatné funkcionality v režime vysokej dostupnosti sú na zvážení uchádzača ako navrhne riešenie tak, aby splnil všetky požiadavky uvedené v opise predmetu zákazky. Zároveň si Vám verejný obstarávateľ dovoľuje uviesť, že v bode 2.11 Opisu predmetu zákazky Prílohy 9 SP je uvedené, že cit.: „Služby sú poskytované minimálne v rozsahu súčasného monitoringu kybernetickej bezpečnosti...“.

Otázka č. 32:
V prílohe 10 SP (Základné informácie o IT prostredí NBS) v bode 5.2 píšete „Počet skenovaných zariadení je približne 680, z toho je cca 1/3 agentových a 2/3 bezagentových zariadení“. V prílohe 9 SP Opis predmetu zákazky , záložka Skenovanie zraniteľnosti, poradové číslo 2.132 píšete“ Cieľové aktíva (skenované systémy): všetky servery, sieťové zariadenia, appliances, pripojené do LAN NBS, vrátane virtualizačných platforiem, databázových platforiem, virtuálnych serverov a kontajnerov prevádzkovaných na virtualizačných platformách ako aj serverov a zariadení spravovaných NBS v cloude. Predmetom služby nie sú koncové zariadenia používateľov (NTB, PC, mobilné zariadenia a pod.).“
Otázka: Z dôvodu nejednoznačnosti z týchto dvoch podkladov, aby sme vedeli správne nacetiť službu sa pýtame: koľko assetov objednávateľ požaduje skenovať?

Odpoveď:
Verejný obstarávateľ si Vám týmto dovoľuje uviesť, že v bode 7.6 v prílohe 10 SP (Základné informácie o IT prostredí NBS) je uvedený súčasný počet Tenable licencií pre **800 IP adries**.

Mgr. Karol Ivančík
Právny expert pre obstarávanie

JUDr. Zuzana Jánošová
Vedúca, oddelenie centrálneho obstarávania

Mgr. Tomáš Lepieš
Riaditeľ, odbor hospodárskych služieb