Město Šumperk
Městský úřad Šumperk
nám. Míru 1, 787 01 Šumperk

Naše čj.: MUSP 46399/2017
Naše sp. zn.: 37299/2017 TAJ/PAKO

* M U S P X 0 I Q Y 6 M N *

Výzva k podání nabídek na veřejnou zakázku malého rozsahu na dodávky

V souladu s ustanovením § 31 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, není tato veřejná zakázka malého rozsahu zadávána podle zákona o zadávání veřejných zakázek.

Název výběrového řízení

Zvýšení zabezpečení počítačové sítě MěÚ Šumperk - část 3. " Monitorovací systém provozu na počítačové síti MěÚ Šumperk "

Číslo výběrového řízení

P17V00000040

Zadavatel, kontaktní osoba

Název:	Město Šumperk
Právní forma:	801 - Obec nebo městská část hlavního města Prahy
Sídlo:	78701 Šumperk, nám. Míru 364/1
Kód ORP:	7111
datová schránka:	8bqb4gk
tel.:	+420 583 388 111
fax.:	+420 583 214 188
IČ:	00303461
DIČ:	CZ00303461
Starosta:	Mgr. Zdeněk Brož
Bankovní spojení:	Česká spořitelna Šumperk, 27-1905609309/0800
Kontaktní osoba:	Ing. Pavel Kouřil
Telefon:	+420 724 189 281
E-mail:	kouril@sumperk.cz

Datum a způsob zveřejnění výběrového řízení

Zaslána vybraným zájemcům prostřednictvím certifikovaného elektronického systému E-ZAK na profilu zadavatele nejpozději dne 15.5.2017

Popis předmětu výběrového řízení - předmět zakázky

Předmětem zakázky je komplexní dodávka a implementace nástroje pro ochranu integrity komunikačních sítí, monitorovací systém, který bude umožňovat dlouhodobé detailní monitorování provozu na počítačové síti Města Šumperka resp. MěÚ Šumperk pro zajištění detekce kybernetických bezpečnostních událostí.

Bankovní spojení: Česká spořitelna
č. ú.: 1905609309/0800
IČ: 00303461
www.sumperk.cz
posta@sumperk.cz
ID datové schránky: 8bqb4gk

Požadavky na řešení

Navržené řešení musí pokrýt jak HW, tak SW a licenční potřeby zadavatele v této věci a musí obsahovat vše potřebné pro zhotovení bezvadného díla odpovídajícího uvedené specifikaci, a to včetně implementace v prostředí zadavatele a v souladu s jeho pokyny.

Požadavky na monitorovací systém

Monitorovací systém musí umožňovat dlouhodobé detailní monitorování provozu na počítačové síti MěÚ Šumperk. Získané statistiky o provozu datové sítě musí umožnit v reálném čase sledovat a vyhodnocovat objemy a strukturu provozu, analyzovat příčiny provozních nebo výkonnostních problémů a odhalovat bezpečnostní hrozby. Je nezbytné, aby monitorovací systém byl zcela nezávislý na použité síťové infrastruktuře a svou funkcí monitorovanou síť neovlivňoval. Ze strany sledované sítě nesmí být monitorovací systém detekovatelný.

Monitorování provozu požadujeme provádět na úrovni dvou hlavních lokalit MěÚ Šumperk propojených optickým single mode kabelem. Vzhledem k současnému maximálnímu vytížení centrálních aktivních prvků provozem v řádech jednotek gigabitů za sekundu musí systém umožňovat přímé monitorování provozu každé z lokalit rychlostí s rozhraním 10 Gbps z jednotlivých centrálních aktivních prvků v každé z lokalit. V případě využití vzdáleného monitoringu toků prostřednictvím samostatných, ale maximálně 2 vyhrazených optických vláken single mode mezi monitorovanými lokalitami. Systém musí zároveň umožňovat jednoduché (konfigurační) přesunutí nebo rozšíření monitorování provozu (monitoringu toků) o monitorování dalších, jak podružných lokalit, tak například o monitorování toků na vstupu z internetu.

Uložení a zpracování informací o provozu – o tocích, musí být prováděno na k tomu určených prostředcích – kolektorech. Ty musí být vybaveny SW či HW RAIDem, případně provozovány na virtualizované infrastruktuře. Kolektory musí poskytovat grafické uživatelské rozhraní a analytické nástroje pro práci se síťovými statistikami bez nutnosti instalovat jakýkoliv software na klientské stanice a dále pak poskytovat automatizované reporty i notifikace na nestandardní situace. Ukládání dat musí probíhat kontinuálně s maximální dostupností a bez jakékoliv ztrátové agregace po dobu několika měsíců. Samozřejmostí je plná customizace způsobu prezentace dat a reportů na základě prostředí sítě MěÚ Šumperk.

Systém musí pracovat s technologií datových toků (NetFlow/IPFIX/jFlow/NetStream/cflow), jelikož tato technologie představuje jak ověřený, tak zároveň nejmodernější prostředek pro monitorování sítě a nabízí výhody zpracování všech paketů bez vzorkování, imunitu vůči šifrovanému provozu, škálovatelnost i pro vysokorychlostní sítě nebo specializovaná prostředí průmyslových sítí.

Požadavek	Popis
Ucelený, škálovatelný NetFlow/IPFIX monitorovací systém	Ucelené škálovatelné řešení umožňující dlouhodobé monitorování sítě na bázi technologie datových toků (NetFlow, IPFIX, jFlow, cflowd, NetStream).
Podpora infrastruktury	Podpora IPv4, IPv6, VLAN, MPLS, Ethernet 10Mb/s až 100Gb/s.
Decentralizovaný monitoring lokalit s centrální správou	Sběr síťových statistik ze vzdálených lokalit s centrálním přístupem k reportům, incidentům a síťovým statistikám a centrální správou systému.
Nezávislost na stávající infrastruktuře	Nezávislost na stávající síťové infrastruktuře (optické či metalické datové rozvody) a použitých aktivních prvcích (typ nebo výrobce).
Zdroje NetFlow statistik	Specializovaná dedikovaná zařízení pro vytváření detailních statistik IP toků o dění na síti, standardizovaný protokol pro výměnu dat o IP tocích (NetFlow v5,v9, IPFIX)
Bezeztrátový sběr flow statistik z více zdrojů	Bezeztrátový sběr dat na kolektorech z různých datových zdrojů, podpora standardizovaných protokolů pro výměnu dat o IP tocích (NetFlowv v5, NetFlow v9 – RFC3954, IPFIX, jFlow, cflowd, NetStream).
Ukládání statistik a vyhodnocování bezpečnostních hrozeb	Dlouhodobé ukládání statistik IP toků a jejich centrální sledování a vyhodnocování bezpečnostních hrozeb v síti, prokazování bezpečnostních incidentů.
Zákaznická podpora	Plná zákaznická podpora v českém jazyce.
Reference	Systém ověřený instalacemi v rozsáhlé síťové infrastruktuře (datové linky 10 Gbps a výše). Minimálně 10 instalací ve třech zemích světa.
Rozhraní pro integraci nástrojů třetích stran	Otevřené rozhraní a dokumentované API s možností integrace nástrojů i třetích stran.

1. Požadavky na zdroje NetFlow/IPFIX dat

Zdroje NetFlow/IPFIX dat musí být výkonná autonomní zařízení, která monitorují síťový provoz, vytváří o něm statistiky v podobě IP toků (NetFlow/IPFIX data) a zasílají tyto statistiky na kolektor pro uložení a další zpracování. NetFlow/IPFIX data musí obsahovat informace o tom, kdo komunikoval s kým, jak dlouho, jakým protokolem, kolik přenesl dat a další informace ze síťové (L3) a transportní (L4) vrstvě OSI modelu. Zařízení (zdroje) rovněž musí umožnit analýzu aplikační vrstvy (L7), identifikaci aplikací (NBAR2) a podrobný monitoring hlavních aplikačních protokolů (např. HTTP, DNS, DHCP, SMB). Mimo objemových charakteristik provozu musí poskytovat zdroje dat rovněž výkonové parametry datové sítě (např. RTT, SRT, jitter) pro analýzu zpoždění na síti a přinášet tak komplexní přehled a detailní informace o dění v síti a usnadňovat tak řešení síťových problémů, správu a optimalizaci sítě a zvyšuje její bezpečnost.
Zdroje dat musí být nezávislé na použité síťové infrastruktuře a svou funkcí nesmí nijak ovlivňovat sledovanou síť. K síti mohou být připojeny pasivně prostřednictvím SPAN/mirroring portu nebo pomocí pasivních rozbočovačů. Ze strany monitorovacích rozhraní připojených do sledované sítě nesmí být zařízení detekovatelné.

Název požadavku	Popis požadavku
Pasivní zapojení	Pasivní zapojení bez vlivu na monitorovanou síť (zapojení pomocí pasivních rozbočovačů, případně v kombinaci se SPAN/mirror porty).
Instalace	Snadná instalace do stávající síťové infrastruktury – racková montáž nebo šablony pro nasazení virtuálního stroje.
Management rozhraní	Dva plnohodnotné management (administrativní) porty 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu a přenos NetFlow dat.
Zabezpečená vzdálená správa	Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS.
Správa uživatelů a přístupových práv	Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí.
Monitorovací linka	Umožňuje připojení SFP+ modulů pro monitorování přes jednovidovou nebo vícevidovou optickou linku.
Dohled	Zařízení je možné integrovat do dohledového systému pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP.
Časová synchronizace	Časová synchronizace zařízení proti centrálnímu zdroji času na síti.
Minimální výkon	Minimální výkon 1,3 milionů paketů za sekundu na každém portu, možnost upgradu na verzi s wire-speed garancí zpracování všech paketů.
Podpora příkazové řádky	Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky. Základní správa prostřednictvím příkazové řádky.
Sériová linka pro konfiguraci zařízení	Možnost přístupu a konfigurace hardwarových zařízení prostřednictvím sériové linky (RS-232).
DNS cache	Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména.
LDAP autentizace	Podpora autentizace vůči LDAP (Active Directory).
TACACS+ autentizace	Podpora autentizace vůči TACACS+
Podpora protokolů pro výměnu dat	Programové vybavení zařízení musí umožnit vytváření NetFlow dat ve formátech verzi 5 a 9, IPFIX.
Zpracování datového provozu	Zpracování datového provozu IPv4 a IPv6, VLAN, MPLS a jejich reportování na kolektor.
Analýza tunelovaného provozu	Monitorování provozu v tunelu GRE.
Uživatelsky definované šablony	Uživatelsky definovatelné šablony pro protokoly NetFlow v9 a IPFIX.
Monitorování MAC adres	Monitorování a reportování MAC adres ve flow statistikách. Možnost použít MAC adresu jako položku klíče flow záznamu.
Detekce aplikací	Detekce aplikací dle standardu NBAR2.
Analýza zpoždění na síti	Reportování RTT, SRT, delay, jitter, retransmise, out-of-order pakety jako součást flow statistik. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).
Monitorování a analýza HTTP provozu	Monitorování a analýza HTTP provozu - včetně položek typu URL, hostname. Pro HTTPS reportování hostname jako SNI. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).
Profilování zařízení v síti	Identifikace operačního systému vč. jeho verze. Identifikace internetového prohlížeče vč.

	jeho verze. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).
Monitorování VoIP	Monitorování VoIP statistik, protokol SIP – položky typu SIP URI, jitter, latence, ztrátovost paketů. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).
Monitorování DNS provozu	Monitorování a analýza DNS provozu - položky jako typ dotazu, dotazovaná doména, návratová hodnota, odpověď. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).
Monitorování SMB/CIFS provozu	Monitorování a analýza SMB/CISF provozu – položky typu síťová cesta, název souboru, typ operace. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).
Monitorování DHCP provozu	Monitorování DHCP provozu – položky jako typ DHCP požadavku, originální MAC adresa. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).
Monitorování rozšířených L3/L4 informací	Monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících detekci NATů.
Kapacita paměti současných toků	Minimální kapacita paměti současných toků na zdroj dat 3,5 milionu toků pro každý monitorovací port.
Nastavení času pro expiraci toků	Podpora pro nastavení časů u aktivní a neaktivní expirace toků.
Vzorkování	Podpora vzorkování na úrovni paketů. Podpora vzorkování na úrovni toků.
Simultánní export NetFlow statistik	Podpora simultánního exportu flow statistik na libovolný počet cílů (redundantní kolektory v různých lokalitách, lokální uložení dat na zařízení). Pro různé cíle exportu lze použít různé flow standardy (NetFlow v5, NetFlow v9, IPFIX).
Export na základě filtrování dat	Podpora filtrování dat na zařízení na základě IP prefixů, VLAN, AS (pro různé cíle exportu různé statistiky).
Vyplňování identifikace AS	Podpora vyplňování AS na základě vestavěného či dodaného seznamu.
Vyplňování čísla interface	Podpora pro nastavení hodnoty interface index pro exportované flow statistiky per monitorovací port.
Záchyt provozu v plném rozsahu	Zařízení umožňuje rozšíření o funkcionalitu záznamu provozu v plném rozsahu na základě uživatelem definovaného pravidla záchytu. Rozšíření je řešeno formou licence/instalace SW bez nutnosti změny HW konfigurace.
Podpora vysokorychlostních sítí	Řešení podporuje sítě s rychlostmi 1/10 (Gigabit Ethernet).
Monitorovací porty zařízení	Zařízení obsahuje minimálně 2x 10GbE monitorovací port na zařízení.

2. Požadavky na kolektor NetFlow dat

Kolektory jsou zařízení/prostředky (datová úložiště) s diskovou kapacitou určená pro uložení, vizualizaci a vyhodnocení síťových statistik exportovaných NetFlow/IPFIX dat.
Zobrazení uložených flow dat a jejich analýza (vyhledávání, agregace, výpisy aj.) musí probíhat na kolektoru prostřednictvím zabezpečeného webového rozhraní HTTPS. Uložená data a výsledky analýz musí být dostupná ve formě dlouhodobých grafů a top statistik s možností zobrazení dat až na úrovni jednotlivých komunikací (jednotlivé NetFlow/IPFIX záznamy). Kolektor dále musí poskytovat funkce reportování statistik o síťovém provozu a systém notifikací v případě výskytu definované události/anomálie. Kolektor tak musí přinášet kompletní přehled o dění v síti a umožňovat operátorům přesně, rychle a efektivně řešit problémy v síti, zvýšit jejich bezpečnost díky detekci analýze provozu, optimalizovat síť, plánovat budoucí rozvoj a kapacitní požadavky a snížit provozní náklady.
Funkčnost kolektoru musí být možno dále rozšířit o systémy pro automatické vyhodnocování NetFlow/IPFIX dat, záchyt síťového provozu, monitorování výkonu aplikací a systémem pro ochranu proti DoS/DDoS útokům.

Název požadavku	Popis požadavku
Ukládání flow statistik	Zabezpečené kolektory flow statistik s databází pro plné uložení síťových statistik na multigigabitových linkách bez jakékoliv redukce.
Granularita vizualizace	Kolektor umožní zpracování a vizualizaci flow záznamů volitelně v 5-minutových nebo 30-sekundových intervalech, přičemž tuto hodnotu lze samostatně nastavit per definovaný síťový rozsah nebo definovanou množinu toků.
Podpora standardů datových toků	Podpora standardů NetFlow v5, NetFlow v9, IPFIX
Hlavní funkcionalita	Možnost dohledání libovolné komunikace až na úroveň jednotlivých flow záznamů, průběžné grafy provozu, top statistiky, reporty, alerty, databáze aktivních zařízení na síti vč. identifikace zařízení.
Instalace	Snadná instalace do stávající síťové infrastruktury – racková montáž nebo šablony pro nasazení virtuálního stroje.
Management rozhraní	Dva management (administrativní) porty 10/100/1000Mb/s pro zabezpečenou vzdálenou správu a přenos NetFlow dat.
Zabezpečená vzdálená správa	Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS.
Správa uživatelů a přístupových práv	Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. Separace dat s omezením přístupu pro jednotlivé role/uživatele.
LDAP autentizace	Podpora autentizace vůči LDAP (Active Directory).
TACACS+ autentizace	Podpora autentizace vůči TACACS+.
Dohled	Kolektor je možné integrovat do dohledového systému pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP.
Časová synchronizace	Časová synchronizace zařízení proti centrálnímu zdroji času na síti.
Podpora příkazové řádky	Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky. Základní správa prostřednictvím příkazové řádky.
DNS cache	Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména.
Podpora položek proměnlivé délky	Podpora IPFIX položek proměnlivé délky.
Monitoring výkonu sítě	Sběr a analýza RTT, SRT, delay, jitter, retransmise, out-of-order pakety.
Monitoring informací z aplikační vrstvy	Podpora pro protokoly HTTP, VoIP SIP, DNS, SMB/CIFS, DHCP, Email, SQL
Monitorování rozšířených L3/L4 informací	Podpora pro monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících identifikaci NATů.
Kapacita datového úložiště	Disková kapacita datového úložiště minimálně 400 GB pro ukládání záznamů a statistik bez jakékoliv redukce v horizontu minimálně šesti měsíců.
Přeposílání flow vč. možnosti samplingu	Možnost přeposílání přijímaných flow statistik ke zpracování na další kolektory včetně možnosti samplování na úrovni datových toků.
Spolehlivý a šifrovaný přenos IPFIX dat	Přeposílání IPFIX dat pomocí spolehlivého TCP spojení s možností šifrování (TCP/TLS).
Automatická identifikace zdroje flow statistik	Kolektor automaticky identifikuje každý zdroj flow statistik, který mu tyto statistiky zasílá ke zpracování. O daném zdroji získá základní informace jako název, počet a rychlost rozhraní. Pro každý zdroj flow statistik automaticky zobrazuje graf průběhu provozu.

Zálohování a obnova flow statistik	Flow statistiky je možné automaticky zálohovat na externí síťové úložiště z důvodu dlouhodobé archivace. Zálohované statistiky lze v případě potřeby přímo obnovit uživatelem do kolektoru, kde je možné tyto statistiky analyzovat standardními prostředky.
Podpora pro uživatelské identity	Kolektor umožňuje zobrazení přihlášeného uživatele u daného zařízení (IP adresy) včetně historie. Flow statistiky je možné filtrovat na základě loginu uživatele. Uživatelské identity jsou získávány ze systémů řízení přístupu do sítě (např. Cisco ISE) nebo Active Directory. Řešení je otevřené a schopné podporovat libovolný zdroj uživatelských identit (hlášení o úspěšné autentizaci uživatele).
Uživatelské rozhraní	Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard s podporou více záložek (konfigurace per uživatel).
Vizualizace statistických dat	Vytváření dlouhodobých grafů a přehledů s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (HTTP, IMAP, SSH), včetně plné konfigurace grafů a pohledů uživatelem.
Analýza dat a ad hoc výstupy	Generování statistik a podrobných výpisů nad volitelnými časovými intervaly s volitelnými filtry. Různé formáty výstupů, minimálně PDF, CSV.
Reporting	Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Koláčové i průběhové grafy. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF nebo CSV. Automatická distribuce reportů e-mailem. Možnost automatického ukládání reportů na externí síťové úložiště.
Řízení uživatelského přístupu	Řízení uživatelského přístupu k jednotlivým typům reportů (uživatel je oprávněn zobrazovat pouze statistiky, ke kterým mu bylo nastaveno oprávnění administrátorem).
Top N statistiky	Výpis tzv. top N statistiky podle různých kritérií (počet přenesených bytů, paketů, toků, nejvyšší hodnoty RTT, průmětné hodnoty SRT, atd.) umožňující vypsat nejaktivnější či anomální počítače podílející se na síťovém provozu.
Filtrování a přizpůsobení výstupů	Systém umožňuje filtrovat s využitím libovolných atributů flow statistik vč. L7 rozšíření nebo výkonnostních parametrů sítě. Filtry je možné kombinovat prostřednictvím logických spojek AND, OR, NOT. Výstupy je možné formátovat, zejména zahrnovat do zobrazení jednotlivé atributy flow záznamů nebo používat řazení (např. dle objemu přenesených dat, dle času nebo dle výkonnostních parametrů datové komunikace).
Uživatelsky definovatelné alerty	Automatická notifikace v případě vzniku uživatelem definované situace (např. nadměrný přenos dat, překročení definované relativní nebo absolutní prahové hodnoty, atd.) prostřednictví emailu, SNMP trapu a syslogu, možnost automatického spuštění uživatelem definovaného skriptu.
Uživatelsky definované pohledy na datový provoz	Uživateli je umožněno definovat si vlastní perzistentní pohledy na data, které budou systémem kontinuálně aktualizovány. K definici pohledu je možné použít libovolný filtr (komunikace daného síťového segmentu, download a upload na server podnikové aplikace, protokol HTTP, apod.).
Drill-down	Možnost dohledat každý jednotlivý datový tok (flow záznam).
Monitoring aktivních zařízení na síti	Monitorování zařízení připojených k datové síti, dlouhodobá historie aktivních zařízení, identifikace na základě IP adresy, MAC adresy, sledování VLAN, operačního systému, přihlášeného uživatele na daném zařízení.
Automatická podpora geolokace	Systém automaticky obohacuje přijímané flow statistiky na základě IP adresy. Provoz je možné filtrovat na základě dané geografické lokality (státu/země).
Otevřené rozhraní	Kolektor poskytuje dokumentované API pro získávání a zpracování dat. Prostřednictvím API je možné kolektor rovněž konfigurovat (např. definovat vlastní pohledy, reporty, apod.).
Aplikace pro mobilní zařízení	Aplikace pro mobilní zařízení platformy Android a iOS, pro zobrazování základních informací v podobě grafů a statistik per jednotlivý uživatel.
Monitorování dostupnosti zdroje flow dat	Monitorování dostupnosti zdroje flow dat pomocí SNMP.

3. Požadavky na automatické vyhodnocování NetFlow dat

Systém pro automatické vyhodnocování IP toků musí umožnit automatickou detekci bezpečnostních nebo provozních a anomálií datové sítě a jejich hlášení formou událostí. Systém by měl být založen na pokročilých metodách tzv. behaviorální analýzy a umožňuje tak odhalovat hrozby a incidenty, které překonaly zabezpečení na perimetru nebo bezpečnostních ochranu koncových stanic, a pro které dosud není dostupná signatura. Jedná se tak o systém včasné detekce a reakce na bezpečností incidenty, který vhodným způsobem doplňuje stávající nástroje pro předcházení kybernetickým bezpečnostním incidentům. Detekované události musí být možné dále analyzovat, vizualizovat nebo automaticky reportovat, případně integrovat například s dohledovými systémy, incident handling systémy a systémy typu SIEM. Automatická detekce bezpečnostních incidentů, anomálií provozu sítě a konfiguračních problémů musí svým chováním výrazně zjednodušit správu datové sítě, zvýšit její bezpečnost a umožnit proaktivně identifikovat příčiny problémů.

Název požadavku	Popis požadavku
Podpora flow standardů	Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream.
Deduplikace	Systém umožňuje deduplikovat flow statistiky před jejich vlastní analýzou.
Korelace před a za proxy	Systém umožňuje provést korelaci flow statistik před a za proxy serverem před jejich vlastní analýzou s cílem identifikovat provoz procházející proxy serverem a tento provoz přiřadit koncovému uživateli.
Vzorkování na úrovni toků	Systém podporuje vzorkování na úrovni toků před jejich vlastním zpracováním až do kapacity 1000 toků/s
Identita uživatelů	Systém zobrazuje informace o identitě uživatelů obsaženou ve flow datech jako součást události.
Persistence doménových jmen	Systém podporuje persistenci doménových jmen, tedy uložení doménové jména původce události v okamžiku zaznamenání výskytu této události.
Detekční pravidla a algoritmy	Systém obsahuje předdefinovanou sadu detekčních metod a algoritmů pro analýzu flow statistik, detekci bezpečnostních incidentů, provozních problémů a síťových anomálií.
Detekce síťových útoků	Detekce skenování portů, slovníkové útoky, útoky odepření služeb (DoS), útoky na síťové protokoly SSH, RDP, Telnet a další obdobné služby.
Detekce anomálií v síťovém provozu	Detekce anomálií v DNS, DHCP, SMTP, multicast provozu a nestandardní komunikace.
Detekce nežádoucích aplikací	Detekce P2P sítí, a anonymizačních služeb (např. TOR)
Detekce událostí na základě „Threat intelligence“ dat	Systém umožňuje identifikovat bezpečnostní události (např. komunikaci s botnet command & control centry, přístup na phishing servery, apod.) využíváním zdrojů IP a host reputačních databází poskytovaných výrobcem a aktualizovaných nejméně každých 24 hodin. Systém umožňuje zapojit další zdroje IP a host reputačních dat pro automatickou detekci.
Detekce provozních problémů	Detekce nadměrné zátěže sítě, výpadků služeb, chybějících reverzních DNS záznamů, nových a cizích zařízení připojených k síti.
Detekce síťových anomálií	Detekce síťových anomálií na základě predikce budoucího chování sítě s využíváním znalosti historie komunikace.
Konfigurační průvodce	Systém obsahuje konfiguračního průvodce pro nastavení systému při prvním spuštění podle parametrů sítě, do kterého je systém nasazen.
Konfigurace detekčních schopností	Jednotlivé detekční schopnosti je možné konfigurovat a parametrizovat tak, aby bylo dosaženo maximální efektivity a minimálního počtu falešných poplachů. Detekční mechanismy je možné konfigurovat různým způsobem (např. s různou citlivostí) pro statistiky z různých segmentů sítě (např. LAN nebo DMZ).
Detekce NATů	Detekce NATů v síti s využitím rozšířených informací z L3/L4.
Správa filtrů	Systém umožňuje definovat filtry vč. komplexních filtrů složených z dílčích filtrů. Pro zjednodušení definice filtrů je možné používat operace jako inverze nebo rozdíl filtrů. Filtry je možné exportovat do formátu XML nebo z tohoto formátu importovat.
Správa falešných poplachů	Případné události, které představují falešné poplachy (false positives) je možné odstranit prostřednictvím jednoduché konfigurace pravidel pro vyloučení falešných poplachů dostupné v uživatelském rozhraní.

Definice závažnosti událostí	Předdefinované priority událostí s možností uživatelského nastavení závažnosti událostí na základě IP adresních rozsahů, typů událostí, míst výskytu nebo detailů události. Jedna událost může mít v závislosti na konfiguraci přiřazeno více priorit.
Agregace událostí	Detekované události je možné automaticky agregovat tak, aby související události byly prezentovány v rámci pojmenované hrozby (např. infikované zařízení v síti, chybně nakonfigurované zařízení, používání nevhodných aplikací nebo služeb apod.).
Správa uživatelů a přístupových práv	Správa uživatelů a přístupových práv k událostem prostřednictvím uživatelských rolí. Separace událostí s omezením přístupu pro jednotlivé role/uživatele.
E-mailové notifikace	Notifikace o detekovaných událostech prostřednictvím e-mailu s podporou různých formátů (HTML, incident handling systém, úsporný textový formát). Možnost připojit vzorek flow dat, na základě kterých byla událost detekována k emailovému reportu.
Uživatelské rozhraní	Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard (konfigurace per uživatel). Vizualizace průběhu provozu s vyznačením detekovaných událostí v závislosti na nastavené závažnosti událostí.
Integrace informací z jiných služeb	Systém integruje informace ze služeb DNS, WHOIS, geolokační služby. Uživatelsky definované externí služby fungující na protokolu HTTP.
Kategorie a komentáře	Události je možné přiřazovat do uživatelsky definovaných kategorií (např. vyřešeno, důležité, apod.). Událostem je možné přímo v systému pořizovat poznámky a komentáře.
Vyhledávání událostí	Systém nabízí flexibilní uživatelské rozhraní pro vyhledávání událostí dle různých parametrů (typ události, IP adrese původce události, filtr, přiřazení události do kategorie, ID události apod.). Události je možné prezentovat různým způsobem (prostý seznam, agregace dle zdrojů, dle cílů apod.).
Interaktivní vizualizace událostí	Systém umožňuje interaktivní vizualizaci detekovaných událostí formou grafické reprezentace flow statistik, na základě kterých byla událost rozpoznána.
Reporting	Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF. Automatická distribuce reportů e-mailem.
CSV export	Události je možné exportovat do formátu CSV pro další zpracování.
Otevřené rozhraní	Systém detekce anomálií poskytuje dokumentované API pro získávání a zpracování událostí. Prostřednictvím API je možné systém detekce anomálií rovněž konfigurovat (např. vytvářet filtry, měnit nastavení detekčních metod, apod.).

4. Požadavky na záchyt síťového provozu

Systém na záchyt síťového provozu umožňuje záznam datového provozu včetně jeho obsahu. Na základě zadaných filtračních kritérií systém provede záchyt síťového provozu, který zpřístupní ve formátu PCAP pro jeho následnou analýzu v libovolných nástrojích třetích stran. Systém tak významně rozšiřuje možnosti v oblasti identifikace a řešení příčin provozních a komunikačních problémů, které jdou za hranici analytických možností IP toků.

Název požadavku	Popis požadavku
Záchyt síťového provozu	Systém zachycuje síťový provoz v plném rozsahu (vrstvy L2-L7) a záznamy zachyceného síťového provozu ukládá v souboru s formátem PCAP, který je možno stáhnout z webového uživatelského prostředí pro následnou analýzu v programu třetí strany (např. Wireshark).
Podpora vysokorychlostních sítí	Systém je schopný záchytu síťového provozu v sítích s rychlostmi až 100Gb/s.
Architektura – distribuovaná	Systémem je možné rozšířit funkcionalitu zdrojů dat. Systém se ovládá centrálně z kolektoru, který obsahuje webové rozhraní pro manuální zadávání požadavků na záchyt síťového provozu. Webové rozhraní kolektoru umožňuje definovat na jakých zdrojích dat a jejich monitorovacích rozhraních bude prováděn záchyt.
Architektura – all-in-one zdroj	Systémem je možné rozšířit funkcionalitu zdroje dat a zároveň jej vybavit webovým rozhraním pro manuální zadávání požadavků na záchyt síťového provozu. Webové rozhraní zdroje dat umožňuje definovat, na jakých monitorovacích rozhraních zdroje bude prováděn záchyt.
Pravidla pro filtraci a záchyt provozu	Systém umožňuje pro jednotlivé záznamy definovat filtry a zachytávat tak část síťového provozu. Kritéria filtrace jsou parametry z vrstev L2-L4 a L7.
Filtrace a záchyt provozu podle parametrů linkové vrstvy (L2)	Systém umožňuje filtrovat síťový provoz podle VLAN tagu, MPLS značky.
Filtrace a záchyt provozu podle parametrů síťové vrstvy (L3)	Systém umožňuje filtrovat síťový provoz podle IPv4, IPv6 adresy, čísla sítě a masky.
Filtrace a záchyt provozu podle parametrů transportní vrstvy (L4)	Systém umožňuje filtrovat síťový provoz podle portů TCP, UDP a SCTP
Nastavení časového intervalu záchytu	Systém umožňuje pro jednotlivé záznamy definovat časový interval, ve kterém se bude síťový provoz zachytávat.
Správa přístupu k záznamům	Systém umožňuje při zadávání záznamu definovat skupinu uživatelů, která má přístup ke stažení záznamu.
Automatické spuštění záchytu provozu	Záchyt síťového provozu je možné spustit automaticky na základě detekce události systémem pro automatické vyhodnocování NetFlow dat.
Definice míst záchytu	Systém umožňuje definovat na jakých zdrojích dat a jejich monitorovacích rozhraních bude provádět záchyt síťového provozu.
Otevřené rozhraní	Systém poskytuje dokumentované API pro získávání záznamů zachyceného síťového provozu. Prostřednictvím API je možné v sytému zadávat požadavky na záchyty síťového provozu a definovat pro ně časový interval a filtrační kritéria.

5. Požadavky na monitorování výkonu aplikací

Systém na monitorování výkonu aplikací poskytuje informace o skutečné odezvě aplikace z pohledu uživatele (tzv. user experience) a to pro všechny uživatele a všechny jejich uživatelské transakce v reálném čase. Systém umožňuje transparentně (bez vlivu na aplikaci a infrastrukturu) a bez instalace softwarových agentů monitorovat provoz aplikace, vyhodnocovat její výkon a reportovat/notifikovat o stavu aplikace. Monitoring probíhá na úrovni uživatel – aplikační server a aplikační server – databázový server. Hlavní metriky jsou doba odezvy a čas na transportní vrstvě, což umožňuje odlišit zpoždění dané zpracováním požadavku od zpoždění přenou dat na síti. Výkon aplikace je možné vyjádřit prostřednictvím ukazatele na bázi tzv. appdexu[1], vypočteného na základě uživatelsky definovaného SLA. Díky tomu je možné přesně identifikovat místa a příčiny problému a tím výrazně zrychlit čas potřebný k jejich nápravě a snížit náklady na správu aplikací.

Název požadavku	Popis požadavku
Uživatelské rozhraní	Webové uživatelské rozhraní v českém jazyce. Vizualizuje stav aplikace pomocí indexu výkonu aplikace, počtu transakcí a dalších informací ve formě grafů a tabulek. Umožnuje analyzovat stav jednotlivých částí aplikace a transakcí.
Uživatelsky definovatelný dashboard	Uživatelsky definovatelný dashboard pro okamžitou vizualizaci stavu aplikace pomocí widgetů. Možnost přizpůsobení a vkládání vybraných widgetů uživatelem, např. index výkonu aplikace, 5 nejpomalejších transakcí, souhrnné informace a další statistiky vztažené k definovatelnému časovému intervalu (předcházejících x hodin/dnů).
Reporting odezvy aplikace	Systém reportuje pro definované aplikace a každou uživatelskou transakci realizovanou nad aplikací dobu odezvy aplikace a čas na transportní vrstvě. Díky tomu je možné odlišit zpoždění sítě od zpoždění aplikace.
Bez-agentní monitoring	Systém monitoruje aplikace bez nutnosti instalovat jakýkoliv SW na servery nebo klientské stanice.
Transparentní monitoring	Systém monitoruje aplikace bez jakéhokoliv vlivu na aplikaci nebo síťovou infrastrukturu.
Architektura systému	Systém je možné nasadit samostatně na jednom zdroji dat, nebo na více zdrojích dat s centrální správou a webovým uživatelským rozhraním na kolektoru.
Monitoring na úrovni uživatel – aplikační server	Systém umožňuje monitorovat komunikaci mezi klienty aplikace a aplikační serverem na bázi protokolu HTTP a HTTPS. V případě použití protokolu HTTPS podporuje automatické dešifrování komunikace se znalostí privátního klíče pro šifrovací protokoly, které toto umožňují.
Monitoring na úrovni aplikační server – databázový server	Systém umožňuje monitorovat komunikaci mezi aplikačními servery a databázovými servery Oracle , MSSQL, Postgre SQL, MySQL MariaDB.
Definice SLA a index výkonu aplikace	Systém umožňuje pro každou aplikaci, resp. i její část definovat SLA pro dobu odezvy. Systém kontinuálně vyhodnocuje všechny transakce a stanovuje celkový index výkonu aplikace na základě plnění SLA.
Konfigurace aplikací	Systém nabízí flexibilní možnosti definice aplikace pro monitoring. Minimálně v rozsahu IP adresy, porty, host, URL vč. regulárních výrazů pro jejich definici.
Korelace	Systém umožňuje korelovat zpoždění na úrovni uživatelské transakce na aplikačním serveru a transakce mezi aplikačním a databázovým serverem. Pro každou uživatelskou transakci je možné zobrazit SQL transakce, které byly v rámci uživatelské transakce vykonány.
Skupiny	Systém umožňuje definovat skupiny pro sledování metrik pouze pro zvolenou podmnožinu transakcí (např. skupina pro PHP soubory, multimediální soubory, část klientů a uživatelů).
Reporting	Systém umožňuje vytvářet reporty dostupné prostřednictvím webového GUI, ve formátu PDF. Reporty je možné automaticky odesílat e-mailem.
Notifikace	Jako reakci na snížení indexu výkonu aplikace, případně další metriky umožňuje systém odeslat e-mail, syslog zprávu, SNMP trap, nebo spustit skript.
Detaily HTTP transakcí	Pro každou transakci jsou dostupné detaily minimálně v rozsahu URL, parametry, user agenty, objem přenesených dat, návratová hodnota, cookie.

[1] https://en.wikipedia.org/wiki/Apdex

Detaily databázových transakcí	Pro každou transakci jsou dostupné detaily minimálně v rozsahu SQL dotazu v plném rozsahu, velikost dotazu a odpovědi, typ SQL dotazu, čas vzniku dotazu i odpovědi a doba odezvy.
Filtrace agregovaných transakcí	Systém umožňuje filtrovat nad seznamem agregovaných transakcí pomocí kritérií (např. APM, index, počet chyb, celkový objem přenesených dat a další). Díky tomu lze získat informace o tom, jaké části aplikace jsou nejpomalejší, vykazují nejvíce chyb, atd.
Filtrace jednotlivých transakcí	Systém umožňuje filtrovat nad seznamem jednotlivých transakcí pomocí různých kritérií (např. IP adresa uživatele, doba odezvy, SLA, uživatelské jméno, začátek a konec transakce a další). Díky tomu lze získat informace o tom, jaká skupina uživatelů komunikovala s aplikací, jaká byla odezva aplikace, pro jaké uživatele a transakce byla aplikace nedostupná, atd.
CSV export	Systém umožňuje exportovat informace o transakcích ve formátu CSV.
Odvozené metriky	Systém sleduje další odvozené metriky jako je průměr, medián, 99-percentil a 95-percentil doby odezvy aplikace, zobrazuje přehled nejpomalejších transakcí, počet uživatelů souběžně pracujících s aplikací, počet transakcí dle splnění SLA, struktura chybových kódů.

6. Požadavky na ochranu před DDoS útoky

Systém na ochranu proti volumetrickým útokům typu DDoS útokům umožňuje rozpoznat volumetrické síťové útoky analýzou flow statistik a na tyto útoky reagovat s cílem ochránit síťovou infrastrukturu a zajistit dostupnost služeb. Systém detekuje volumetrické útoky typu DDoS na základě sledování změn v charakteristikách síťového provozu pro chráněnou infrastrukturu. Charakteristiky síťového provozu systém získává analýzou IP toků a jejich změny vyhodnocuje na základě statických a dynamických pravidel. Systém zaznamenává detekované útoky ve webovém uživatelském prostředí, pomocí kterého lze zobrazit detailní informace a analyzovat útoky. Systém umožňuje na základě detekce útoku vytvořit alert, přesměrovat síťový provoz, spustit uživatelsky definovaný skript a využít služeb a zařízení pro eliminaci útoku (tzv. mitigaci).
Nasazení systému probíhá bez jakýchkoliv změn konfigurace, topologie sítě nebo dodatečných investic do síťových komponent. Systém je možné jej nasadit samostatně, případně ve spolupráci se službou tzv. Scrubbing centra nebo specializovaným řešením pro eliminaci (mitigaci) DDoS útoku nasazeného tzv. out-of-band.

Název požadavku	Popis požadavku
Uživatelské rozhraní	Webové uživatelské rozhraní v českém jazyce. Obsahuje seznam detekovaných útoků a umožňuje konfiguraci systému. Seznam detekovaných útoků poskytuje základní informace o útoku (stav útoku, začátek, konec, název segmentu, provedené akce) a možnost zobrazení detailů útoku a jeho analýzu.
Podpora flow standardů	Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream. Systém dokáže detekovat útoky i ze vzorkovaných flow statistik.
Detaily útoků	Systém poskytuje přehledné a detailní informace o útoku. Uživateli poskytuje informace o stavu útoku, začátku, konci, typu útoku a další informace o útoku (top statistiku cílových IP adres, portů, zdrojových podsítí, autonomních systému, L4 protokoly, kombinací TCP příznaků a další).
Vizualizace útoku	Systém umožňuje vizualizaci útoku pomocí grafu počtu přenesených paketů v čase a prahů pro detekci útoku. Graf je možné zobrazovat pro jednotlivé detekční metody, L4 protokoly a kombinace TCP příznaků.
Analýza útoku	Systém je integrován s kolektorem a umožňuje se přepnout do jeho uživatelského rozhraní pro manuální a podrobnou analýzu útoku.
Nasazení stand-alone	Systém je možné nasadit samostatně na kolektoru pro detekci DDoS útoků.
Přesměrování provozu	Systém umožňuje přesměrovat provoz na základě detekce útoku pomocí technik PBR (Policy Based Routing), BGP (Border Gateway Protocol).
Integrace s out-of-band zařízeními	Systém je možné integrovat s out-of-band zařízeními třetích stran pro mitigaci DDoS útoků.
Integrace se scrubbing centry	Systém je možné integrovat se scrubbing centry třetích stran pro mitigaci DDoS útoků.
Reporty	Detaily útoku a jeho vizualizace je možné exportovat z webového rozhraní ve formě PDF souboru nebo report automaticky zaslat přes e-mail.
E-mail alerty	Detekované útoky je možné notifikovat pomocí e-mailu. Systém má více úrovní notifikace e-mailem – při detekci útoku, v okamžiku, kdy je známá charakteristika útoku a po ukončení útoku.
Syslog a SNMP trap	Detekované útoky je možné notifikovat do dohledových systémů prostřednictvím funkcionality SNMP trap nebo pomocí syslog zpráv.
Spuštění skriptu	Systém umožňuje na základě detekce útoku spustit uživatelův skript.
Statické detekční metody	Systém umožňuje nastavit pravidlo pro detekci útoků jako poměr mezi příchozími a odchozími pakety.
Manuální threshold (práh)	Systém umožňuje uživateli manuálně nastavit threshold (práh) jako % násobek/nárůst kompletního síťového provozu oproti naučené baseline. Uživatel nastavuje délku časového intervalu, po který se systém učí a stanovuje baseline.
Adaptivní threshold (práh)	Systém podporuje metodu adaptivního thresholdu (prahu), kde si systém sám stanoví baseline pro různé typy síťového provozu (provoz TCP, UDP, ICMP a provoz s různými kombinacemi TCP příznaků). Systém je schopen detekovat první útoky do 15ti minut od uvedení do provozu.
Minimální threshold (práh)	Systém umožňuje definovat minimální threshold (práh), který může pracovat ve dvou režimech. V prvním režimu představuje objem provozu, který musí být

	překročen, aby systém začal vyhodnocovat provoz a detekovat útoky podle nastavených metod (statická, manuální threshold, adaptivní threshold). Díky tomu je možné předejít falešným detekcím například při vysoké hodnotě relativního nárůstu provozu nedosahující významné absolutní hodnoty. V druhém režimu představuje úroveň provozu, při jejímž dosažení je vždy detekován útok.
Definice chráněných segmentů	Systém umožňuje definovat segmenty, čili části sítě (podsítě), pro které budou kontinuálně vyhodnocovány specifické baseliny a detekován útok. Segmenty se definují IP adresními rozsahy.
Definice směrovačů	Systém umožňuje definovat, jaké směrovače a metody pro změnu směrování budou použity při detekci útoku.
Začátek mitigace	Systém umožňuje manuální nebo automatické spuštění mitigace a definování podsítí a IP adres, pro které bude útok mitigován.
Log mitigačního procesu	Systém zobrazuje informace o průběhu mitigačního procesu a (ne)úspěšnosti jeho nastartování. Díky tomu je možné zjisti přesné místo selhání a urychlit tak troubleshooting.
Mitigace útoku	Systém podporuje BGP Flowspec standard pro eliminaci DDoS útoku pomocí kompatibilního směrovače. Systém vytváří dynamickou signaturu probíhajícího útoku a předává ji směrovači, jenž pro provoz odpovídající signatuře provede uživatelem definovanou akci.
Automatická detekce cílových IP/podsítí útoků pro mitigaci	Systém automaticky detekuje IP adresy nebo podsítě, které jsou postiženy DDoS útokem a umožňuje mitigaci specifických IP adres z chráněného segmentu, části chráněného segmentu nebo celého chráněného segmentu.
Rychlost detekce DDoS útoku	Systém detekuje útok do 60 sekund (nejhorší případ) od začátku útoku.

Termín a místo plnění zakázky

Předpokládaný termín zahájení plnění: ihned po podpisu smlouvy
Nejzazší termín ukončení plnění: 30. 11. 2017
Místo plnění: Obec s rozšířenou působností Šumperk

Dodatečné informace k výzvě

Uchazeč je oprávněn požadovat po zadavateli dodatečné informace k výzvě k podání nabídek.
Lhůta pro dotazy: nejpozději 3 dny před lhůtou pro podání nabídek.
Dotazy adresujte pouze písemně elektronicky na profilu zadavatele prostřednictvím sytému E-ZAK.
Byla-li žádost o dodatečné informace k výzvě doručena ve stanovené lhůtě, je zadavatel povinen poskytnout uchazeči dodatečné informace. Dodatečné informace, včetně přesného znění žádosti, poskytne zadavatel i všem ostatním uchazečům.

Lhůta, místo a forma pro podání nabídek

Místo: Nabídku uchazeč podá prostřednictvím elektronického systému E-ZAK na profilu zadavatele. URL adresa této zakázky je https://zakazky.sumperk.cz/vz00000729
Lhůta: 24.5.2017 do 10:00 hod
Forma: Nabídka uchazeče bude ve formě pdf souboru(ů).

Zadávací lhůta

Délka zadávací lhůty činí 30 kalendářních dnů. Zadávací lhůta začíná běžet okamžikem skončení lhůty pro podání nabídek a končí dnem doručení oznámení zadavatele o výběru nabídky. Uchazečům, s nimiž může zadavatel uzavřít smlouvu, se zadávací lhůta prodlužuje až do uzavření smlouvy nebo do zrušení zadávacího řízení.

Předpokládaný termín oznámení výsledků výběrového řízení

Předpokládaný termín oznámení výsledků výběrového řízení: 29.5.2017

Požadavky na zpracování nabídky

Nabídka bude zpracována dle formálních, technických a smluvních požadavků zadavatele uvedených této výzvě k podání nabídky.

Členění nabídky

Nabídka musí obsahovat následující kapitoly:

1. Titulní list nabídky
2. Obsah nabídky s uvedením čísel stran
3. Doklady ke splnění kvalifikačních předpokladů
4. Předmět nabídky
5. Cenová nabídka
6. Termín plnění
7. Návrh smlouvy o dílo
8. Přílohy (nepovinné)

Titulní list, podmínky platnosti a závaznosti nabídky

Nabídka na titulním listu musí obsahovat datum.
Uchazeč podá pouze jednu nabídku a nesmí být současně dodavatelem jiného uchazeče v tomtéž zadávacím řízení. V případě porušení této podmínky budou všechny nabídky obsahující tohoto uchazeče vyřazeny.
Dodavatel, který nepodal nabídku v zadávacím řízení, však může být dodavatelem více uchazečů v tomtéž zadávacím řízení.

Kvalifikační předpoklady

Zadavatel požaduje v nabídce doložit kopii příslušného oprávnění k podnikání, a to výpis z živnostenského rejstříku a výpis z obchodního rejstříku (v případě, je-li uchazeč do tohoto rejstříku zapsán), výpis z obchodního rejstříku nesmí být starší 90-ti dnů ke dni podání nabídky.

Vybraný uchazeč o veřejnou zakázku zadavateli před podpisem smlouvy o dílo předloží originál nebo úředně ověřenou kopii oprávnění k podnikání ne starší 90-ti dnů.

Zadavatel požaduje doložení seznamu 3 obdobných významných zakázek uchazeče za poslední 3 roky formou čestného prohlášení. Seznam bude obsahovat označení zadavatele, rok zpracování, cena, název zakázky a kontakt na zadavatele.

Požadavky na zpracování nabídkové ceny

Uchazeč stanoví nabídkovou cenu za provedení veřejné zakázky v souladu s podmínkami veřejné zakázky uvedené v této výzvě k podání nabídky a to absolutní částkou v českých korunách. Nabídková cena bude uvedena jako nejvýše přípustná a musí obsahovat veškeré náklady nutné k realizaci zakázky. Členění nabídkové ceny

- Celková nabídková cena bez DPH

- DPH
- Celková nabídková cena včetně DPH

Požadavky na vyhotovení a úpravu nabídky

Jazyk nabídky

Nabídka i veškeré další doklady požadované zadávacími podmínkami musí být předloženy v českém jazyce. Doklady, kterými zahraniční osoba prokazuje splnění kvalifikace, musí být předloženy v původním jazyce a též v úředně ověřeném překladu do českého jazyka.
Zjistí-li se rozdíl v obsahu, je rozhodující překlad v českém jazyce.

Úprava nabídky

Pokud nabídka bude obsahovat přílohy (fotografie, prospekty a další materiály), pak tyto přílohy budou neoddělitelně zařazeny až na konci za vlastní nabídkou uchazeče, jednotlivé přílohy budou postupně číslovány a jednotlivé listy příloh budou rovněž očíslovány v návaznosti na číselnou řadu vlastní nabídky.

Obchodní podmínky

Součástí nabídky bude návrh smlouvy o dílo, který musí akceptovat veškeré požadavky stanovené zadavatelem v podmínkách soutěže a to jak požadavky věcné a technické, tak požadavky právní a smluvní. Návrh smlouvy musí dále obsahovat podmínky, za nichž uchazeč nabízí splnění veřejné zakázky ve své nabídce.
Návrh smlouvy o dílo musí obsahovat zejména:
- označení smluvních stran;
- předmět smlouvy;
- dobu plnění dle výzvy;
- cenu;
- platební podmínky;
- záruční podmínky;
- odpovědnost za vady a nedodělky;
- smluvní pokuty - sankce za neplnění smluvních termínů vztažené k jednomu dni prodlení;
- další ujednání.

Platební podmínky

Cena díla bude fakturována do 14 dnů ode dne protokolárního předání díla.
Objednatel je oprávněn před uplynutím lhůty splatnosti vrátit fakturu - daňový doklad zhotoviteli, pokud neobsahuje náležitosti dle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, nebo obsahuje nesprávné údaje týkající se fakturované částky. Vrácením faktury přestává běžet lhůta její splatnosti. Opravená faktura bude opatřena novou lhůtou splatnosti dle výše uvedeného způsobu fakturace.
Všechny platby se považují za uhrazené ze strany objednatele okamžikem jejich připsání na účet zhotovitele uvedený na faktuře.

Způsob hodnocení nabídek a výběr dodavatele

Základním kritériem pro hodnocení veřejné zakázky je:
- Nabídková cena včetně DPH.

Výdaje spojené s podáním nabídky

Uchazeči nemají právo na úhradu nákladů spojených s účastí v zadávacím řízení a nesou veškeré náklady spojené s vypracováním a podáním nabídky. Zadavatel v žádném případě neponese za takové náklady zodpovědnost, bez ohledu na průběh a výsledek zadávacího řízení. Zadavatel nenese žádnou odpovědnost ani nebude hradit žádné výdaje nebo ztráty, které uchazeči vzniknou v souvislosti s prohlídkou místa plnění či jakoukoli další činností související s podáním nabídky.

Vyhrazená práva zadavatele

a) zadavatel si vyhrazuje právo bez uvedení důvodu zrušit výběrové řízení,
b) zadavatel si vyhrazuje právo ověřit si informace uvedené uchazeči v nabídkách,
c) zadavatel předložené nabídky uchazečům nevrací,
d) náklady spojené se zpracováním nabídek zadavatel uchazečům nehradí,
e) zadavatel si vyhrazuje právo v průběhu zakázky změnit, upřesnit nebo doplnit podmínky zakázky, a to písemně a všem účastníkům zakázky shodně,
f) zadavatel si vyhrazuje právo odmítnout všechny předložené nabídky a neuzavřít s žádným uchazečem smluvní vztah
g) zadavatel si vyhrazuje právo omezit rozsah veřejné zakázky.
h) nesplnění podmínek zadání či neúplnost nabídky je důvodem k vyřazení nabídky z hodnocení a vyloučení uchazeče z další účasti v zadávacím řízení.

V Šumperku, dne 12.5.2017

Za Město Šumperk

Mgr. Zdeněk Brož
starosta