Zadávací dokumentace zakázky

č. 184/14/OCN

Analyzátor zranitelnosti

1. Identifikační údaje zadavatele, základní parametry zakázky

1.1. Identifikační údaje zadavatele

Společnost: ČEPRO, a. s.
Sídlem: Dělnická 213/12 , 170 04 Praha 7
IČ: 601 93 531
DIČ: CZ 601 93 531
zastoupena: Mgr. Jan Duspěva, předseda představenstva
Ing. Ladislav Staněk, člen představenstva

zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 2341

(dále jen „zadavatel“)

1.2. Kontaktní osoby

Zadavatel se zavazuje poskytnout zájemcům informace potřebné pro podání nabídky k této zakázce. Kontaktní osobou ve věcech:
výběrového řízení: Milan Trnka, 221 968 254, milan.trnka@ceproas.cz
technických: Ing. Vladimír Michálek, vladimir.michalek@ceproas.cz, 739 535 764

1.3. Druh řízení

Jedná se o zakázku malého rozsahu na služby ve smyslu ustanovení § 10 a 12 odst. 3 zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů (dále jen „ZVZ“) a dle § 18 odst. 5 ZVZ není zadavatel povinen zadávat zakázky malého rozsahu postupem dle tohoto zákona.

1.4. Vymezení předmětu zakázky

Předmětem této zakázky je poskytnutí služby automatizovaného bezpečnostního testování zranitelností IT/IS systémů společnosti Čepro a.s. (dále jako projekt/řešení bezpečnostního testování a auditu ICT CEPRO), na období 12 měsíců a to formou služby. Bližší specifikace služby je uvedena v čl. 2 této zadávací dokumentace.

1.5. Doba a místo plnění veřejné zakázky

Termín realizace předmětu zakázky tj. služby je předpokládán na období 12 měsíců - od 1. 11. 2014 do 1. 11. 2015.
Místem plnění jsou sklady ČEPRO, a. s. a sídlo centrály zadavatele.

2. Rozsah a technické podmínky

2.1. Rozsah zakázky

S ohledem na rozsah informačních systémů (dále IS) zadavatele musí projekt pokrýt a naplnit minimálně následující hlavní cíle:

a) řešení potřeby automatizovaného periodického testování zranitelností externích systémů IS ČEPRO (přístupných z internetu a veřejných sítí), pokrývající veškerou informační a telekomunikační (dále jen CT) infrastrukturu zadavatele zajišťující zpracování, uchování nebo přenos dat. Požadovaný rozsah je 30 IP adres přístupných z Internetu.
b) řešení potřeby automatizovaného periodického testování zranitelností interních IS ČEPRO (přístupných z interní LAN a WAN ČEPRO), pokrývající veškerou ICT infrastrukturu zadavatele zajišťující zpracování, uchování nebo přenos dat. Požadovaný min. rozsah 2000 interních IP adres.
c) řešení potřeby automatizovaného periodického bezpečnostního auditu konfigurace klíčových externích a interních systémů IS ČEPRO dle doporučení a opatření standardů CIS (Center for Internet Security), ISO/IEC 27001 a PCI-DSS v. 2.0. Dodaný nástroj/služba musí umožňovat také provádění auditů konfigurace dle zákaznicky definovaných bezpečnostních politik a opatření. Požadovaný min. rozsah 120 IP adres.
d) řešení potřeby automatizovaného periodického bezpečnostního testování a auditu webových aplikací IS ČEPRO, provozovaných na externích a interních serverech IS ČEPRO s cílem identifikovat zranitelnosti (dle metodiky OWASP TOP-10) a nebezpečný kód (malware) uvnitř zdrojového kódu web aplikací. Dodaný nástroj/služba musí umožňovat testování a audit zdrojového kódu web aplikací anonymně (bez přihlášení uživatele) a autentizovaně (pod kontem vybraného uživatele aplikace). Požadovaný min. rozsah 10 web aplikací.

e) řešení musí podporovat kontinuální non-stop skenování externích systémů z pohledu zranitelností a neočekávaných změn v podobě nových hostů, nežádoucích operačních systémů, software, otevřených TCP a UDP portů, certifikátů s vypršelou nebo končící platností, s automatizovaným upozorněním určenému okruhu administrátorů systému, v minimálním počtu 30 IP adres přístupných z Internetu.
f) služba bezpečnostního testování a auditu ICT CEPRO musí obsahovat kompletní dodávku a instalaci veškerého potřebného SW a HW vybavení pro naplnění uvedených cílů, včetně konfigurace a zaškolení do obsluhy a údržby dodaného řešení. Implementace musí obsahovat úspěšné provedení akceptačních testů a bezpečnostních auditů vybraných externích a interních systémů a web aplikací IS ČEPRO v rozsahu uvedeném v tabulce v bodu g).
g) Sumarizace požadovaného minimálního rozsahu projektu

	Popis funkce	Požadovaný rozsah	Rozsah pro akceptaci
1	testování zranitelností externích systémů IS ČEPRO	30 IP adres	5 IP adres
2	testování zranitelností interních systémů IS ČEPRO	2000 IP adres	100 IP adres
3	audit konfigurace ext. a int. systémů IS ČEPRO	120 IP adres	5 IP adres
4	testování a audit webových aplikací IS ČEPRO	10 web aplikací	2 web aplikace
5	kontinuální skenování externích systémů IS Čepro	30 IP adres	3 aplikace

2.2. Funkční specifikace testovacích a auditních nástrojů/služby

a) pravidelné automatické i ad-hoc ruční spouštění mapování síťové infrastruktury s identifikací aktivních systémů, jejich OS a vyznačením nových, potvrzených a nepotvrzených zařízení;
b) centrální databáze (asset management) všech zjištěných zařízení, s tříděním dle administrátorsky definovaných příznaků
c) možnost filtrování výsledků síťové infrastruktury dle platformy OS, otevřených TCP-IP portů, potvrzených/nepotvrzených zařízení, srovnávání historických dat s vyznačením rozdílů;
d) detekce zranitelností na vzdáleném ICT zařízení s podporou minimálně následujících operačních systémů (Windows, AIX, Linux), databází (Oracle, MS SQL), firewallů (Cisco) a aktivních síťových prvků (Cisco);
e) pravidelné automatické i ad-hoc ruční spouštění testování zranitelností ICT zařízení v prostředí síťové infrastruktury, s možností výběru IP rozsahu nebo předdefinovaných skupin zařízení a s výběrem/úpravou profilu a zátěže testování;
f) možnosti voleb intenzity testování (kolik IP adres a TCP/UDP portů paralelně), rychlosti testování (port mapping speed, packet delay time) s minimalizací zátěže testovaných zařízení, síťové infrastruktury a analyzátorů zranitelností samotných;
g) minimalizace rizika pádu testovaného zařízení nebo síťové služby na zařízení, možnost zákazu provádění invazivních testů, zákazu aplikace exploitů, DoS, DdoS útoků a pasword brute forcingu;
h) ve výsledcích testování identifikace všech zjištěných zranitelností včetně míry jejich rizikovosti, popisu příslušných TCP/UDP portů, protokolů, síťových služeb a aplikací na kterých byly detekovány;
i) pro každou zjištěnou zranitelnost uvádět popis relevantních hrozeb, možného negativního dopadu na systém, odkazy na další informační zdroje popisující danou zranitelnost (web stránku výrobce SW, CVE.ORG, Buqtraq.ID apod.) a popis odstranění zranitelnosti s uvedením http linku na patch výrobce nebo postup změny konfigurace systému;
j) pro každou zjištěnou zranitelnost uvádět, zda existuje exploit nebo malware (sw kód nebo vir) umožňující manuální nebo automatizované zneužití zranitelnosti. Nástroj musí monitorovat alespoň 1 nezávislou databázi exploitů a alespoň 1 nezávislou databázi malware a zjištěné informace uvádět v popisu nalezených zranitelností.
k) možnost centralizované customizace databáze zranitelností, umožňující pro celý rozsah implementace měnit hodnotu rizikovosti zranitelnosti, popisu jejich hrozeb, negativního dopadu a popisu odstranění zranitelností, možnost centrálně ignorovat a vyjmout zranitelnosti z testování, možnost editace CVSS Scoring;
l) snadný a customizovatelný reporting a filtrování výsledků testování, zpracování trendů za libovolné časové období nad historií testování, porovnávání stavu zranitelností za zvolené časové období a oblast a srovnávání výsledků vybraných historických testů;

m) podrobný technický reporting všech zjištěných zranitelností, informací a detailů o reportovaných systémech s možností filtrování zvolené úrovně a typu detailu. Sumární přehledový management reporting o celkovém stavu a počtu zranitelností, trendem a vyplývající míře rizika nad zvoleným rozsahem reportu;
n) možnost automatického provádění bezpečnostního auditu konfigurace následujících operačních systémů (Windows, AIX, Linux), databází (Oracle, MsSQL) a aktivních prvků (CISCO) vůči šablonám technických bezpečnostních opatření založených na standardech CIS, NIST, ISO 27001, mapovaných na bezpečnostní požadavky standardu PCI-DSS v. 2.0.
o) možnost definovat a vytvářet vlastní bezpečnostní kontroly konfigurace operačních systémů Windows, Linux a Unix na základě vybraných konfiguračních parametrů uložených v registrech a filesystému operačních systémů a možnost kontrolovat integritu vybraných konfiguračních souborů.
p) možnost provádět automatizované testy zranitelností a auditu zdrojového kódu web aplikací anonymně (bez přihlášení uživatele) a autentizovaně (pod kontem vybraného uživatele aplikace). Požadována je detekce zranitelností dle OWASP TOP-10 metodiky, možnost katalogizace rozsahu web aplikací pod kontem uživatele a porovnání přístupových práv uvnitř web aplikace mezi jednotlivými uživateli.

2.3. Technická specifikace testovacích a auditních nástrojů/služby

a) uvedené funkční požadavky musí být splněny pro celý rozsah implementace s centralizovaným managementem, jednotným a systémově a administrativně snadno ovladatelným aplikačním prostředím a centralizovanou databází všech výsledků testování;
b) škálovatelné řešení v prostředí síťové infrastruktury pro libovolný počet lokalit, interních a externích/DMZ segmentů, s možností provádět volitelně testy z Internetu nebo z vybraných interních síťových scannerů s podporou přístupu do VLANs; Možnost fyzicky oddělit aktualizaci databáze zranitelností a scanning engine na interním testovacím zařízení od segmentu pro provádění interních testů;
c) automatická komunikace internet scannerů a interních síťových scannerů s centrální management aplikací a centrální databází profilů a výsledků testování;
d) automatická centrální archivace všech výsledků historických testů zranitelností ze všech testovaných zařízení. Archivace výsledků testů, jako součást služby min.12 měsíců s možností exportu ve formátech XML, CSV, HTM, PDF.
e) periodická automatická aktualizace databáze zranitelností a testovací aplikace (scanning engine) na všech skenovacích zařízení (interních i externích v internetu) musí být garantovaná dodavatelem s 24 hod. reakcí na nově popsané zranitelnosti (jejichž zdroj je uváděn např. na stránkách výrobců SW, CVE.ORG nebo Bugtracq.ID;
f) schopnost provádět centralizované aktualizace databáze zranitelností popř. aktualizace pro analyzátor zranitelností ze vzdálené lokality nebo lokálních souborů, manuálně, automaticky nebo plánovaně;
g) bez-agentní detekce zranitelností bez nutnosti instalace programového kódu na testovaná zařízení. Možnost provádět testování zranitelností bez anebo volitelně s vzdálenou autentizací na testovaných systémech;
h) centralizované a zabezpečené úložiště (ve správě dodavatele) všech výsledků mapování sítě a testování zranitelností systémů s řízením přístupových oprávnění na základě rolí;
i) veškerá zjištěná data o infrastruktuře IS a zjištěné zranitelnosti a informace o testovaných zařízeních musí být v případě, že se generují a/nebo zpracovávají mimo vlastní IT infrastrukturu zadavatele, vždy uložena a přenášena s použitím silného šifrování: pro ukládání dat symetrické šifry s min. 128bit délkou klíče, pro přenášení dat symetrické šifry min. 128bit délkou klíče,
j) volitelnou možnost dokoupení API/XML/SMTP integrace s řešeními třetích stran pro patch management, helpdesk/servicedesk, configuration management, incident a event log management (SIEM)
k) seznamy požadovaných platforem pro testování zranitelností, audit konfigurace – Windows, AIX, LINUX, Oracle, MS SQL, CISCO
l) seznamy požadovaných technik a typů zranitelností pro testování web aplikací – OWASP TOP-10 jako např. XSS, SQL injection, Blind SQL injection, Web traversal
m) projekt musí být řešen v celé své šíři jediným produktem a povaha řešení musí být zcela bez agentní.

2.4. Požadavky na lokální a vzdálený support systému Analyzátoru zranitelností

a) poskytovatelem garantovaný 24x7x365 support formou emailu a telefonického hot-line v českém/anglickém jazyce, s garantovanou dobou odezvy a zahájením řešení problému do 24hod od nahlášení problému;
b) možnost kontaktování supportu poskytovatele a odesílání false-negative a false-positive nálezů.

c) dodavatelem garantovaný vzdálený email support a telefonický hot-line pokrývající standartní pracovní dobu zadavatele (od 9:00 do 16:00) v českém jazyce;
d) dodavatelem garantovaná obnovená funkčnost služby při porušeí do 5 max. prac.dnů od nahlášení závady;
e) podrobná dokumentace uživatelského prostředí a systémového nastavení služby v prostředí objednatele.

2.5. Požadavky na nasazení produktu a součinnost při realizaci projektu

a) zadavatel požaduje 14 denní bezplatný zkušební provoz, kdy se ověří všechny výše uvedené funkčnosti služby dle bodů 2.1 – 2.4 a to minimálně v rozsahu dle bodu 2.1.g. Při jejich splnění bude projekt analyzátoru bezpečnosti akceptován.
b) maximální doba potřebná k nasazení produktu a jeho předání k 14 dennímu bezplatnému zkušebnímu provozu je 1 měsíc od podpisu smlouvy

V celkové nabídkové ceně bude obsažena instalace, nasazení a konfigurace systému a veškeré náklady na zkušební provoz.

3. Požadavky na varianty nabídek

Zadavatel nepřipouští varianty nabídky.

4. Způsob zpracování nabídkové ceny

Nabídkovou cenou se rozumí cena za provádění předmětu této zakázky dle podmínek uvedených v této zadávací dokumentaci a jejích nedílných součástech.

Nabídková cena bude stanovena za kompletní službu dle specifikace uvedené v čl. 2 této zadávací dokumentace a bude rozdělena rovněž do jednotlivých položek dle tabulky v bodu 2.1 písm. g) této zadávací dokumentace, přičemž nabídkovou cenou se rozumí celková cena za službu dodavatele za období 12 kalendářních měsíců.

Nabídková cena bude uvedena v korunách českých bez DPH.

Nabídková cena bude pro uchazeče závazná, musí být definována jako nejvýše přípustná, se započtením veškerých nákladů, rizik, zisku apod. spojených s plněním celého rozsahu zakázky (včetně veškerých dalších nákladů např. dopravy, poplatků, režijních nákladů atd.) na celou dobu a rozsah plnění zakázky.

Výběrové řízení bude realizováno formou více kol a uchazeči budou v každém kole předkládat nové nabídkové ceny, které budou podkladem pro hodnocení nabídek a budou pro uchazeče závazné. Podrobný popis hodnocení nabídek je uveden v článku 5 – Způsob hodnocení nabídek.

5. Způsob hodnocení nabídek

Hodnotícím kritériem je splnění požadavků zadavatele na rozsah a technickou specifikaci a dále nejnižší celková nabídková cena nabídnutá uchazečem. Nabídková cena bude vždy stanovena v Kč bez DPH dle článku 4 této zadávací dokumentace.

Hodnocení nabídek bude probíhat dle níže uvedených pravidel.

Celkový počet hodnotících kol není omezen. Současně s výzvou pro předložení nabídkových cen pro hodnocení v dalším kole může zadavatel uchazeče informovat o tom, že následující hodnotící kolo bude poslední.

Zadavatel může kdykoliv oznámit uchazečům, že v následujícím hodnotícím kole bude omezen počet uchazečů, tzn., že do dalšího hodnotícího kola postoupí pouze přesně určený počet nabídek.

Pro každého uchazeče je vždy závazná poslední předložená nabídková cena.

Jednání s uchazeči bude probíhat prostřednictvím e-mailu, pokud nebudou uchazeči vyzváni k písemnému nebo osobnímu jednání.

V průběhu prvního hodnotícího kola výběrového řízení bude posuzováno splnění kvalifikace jednotlivými uchazeči, a zda jimi předložená technická specifikace splňuje podmínky požadované zadavatelem. Následně

budou úspěšní uchazeči vyzváni k předložení upravených nabídkových cen (a to i na základě upřesnění požadované technické specifikace zadavatelem).

V druhém kole bude sestaveno pořadí nabídek dle nabídkových cen. Zadavatel může již po tomto kole rozhodnout o výběru nejvhodnější nabídky. Neučiní-li tak, informuje uchazeče o zahájení dalšího kola hodnocení a zároveň je vyzve k předložení nabídkových cen pro další kolo hodnocení. Tento postup platí stejně pro všechna následující kola.

Uchazeč, který bude v posledním kole vyhodnocen jako vítězný, bude vyzván k podpisu smlouvy. Neposkytne-li vítězný uchazeč dostatečnou součinnost k podpisu smlouvy, a ta nebude z důvodů na jeho straně podepsána do 15 dnů od vyzvání k jejímu podpisu, může zadavatel vyzvat k podpisu smlouvy uchazeče, který se v konečném hodnocení umístil na druhém místě (to stejné platí i pro další uchazeče v pořadí).

6. Obchodní podmínky včetně platebních

6.1. Smluvní podmínky

Detailní smluvní podmínky jsou uvedeny v návrhu smlouvy, jenž je přílohou č. 1 této zadávací dokumentace. Návrh smlouvy je pro dodavatele závazný.

6.2. Platební a fakturační podmínky ve znění návrhu smlouvy

a) Zadavatel neposkytuje zálohy.
b) Podkladem pro zaplacení sjednané ceny je vždy daňový doklad – faktura, který vystaví dodavatel v souladu s podmínkami uvedenými v návrhu smlouvy, jenž je přílohou č. 1 této zadávací dokumentace.
c) Splatnost každého daňového dokladu – faktury je 30 dnů ode dne jejího prokazatelného doručení zadavateli.
d) Daňový doklad – faktura musí obsahovat veškeré náležitosti daňového dokladu podle příslušných ustanovení zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění, a další náležitosti požadované zadavatelem. Platba za předmět plnění bude probíhat bezhotovostním převodem z účtu zadavatele na účet dodavatele. Dodavatel musí mít veden účet u peněžního ústavu v České republice. Číslo účtu musí být uvedeno též na faktuře – daňovém dokladu vystaveném dodavatelem.
e) Bližší platební a fakturační podmínky jsou uvedeny v návrhu smlouvy, jenž je přílohou č. 1 této zadávací dokumentace.

7. Podmínky a požadavky na zpracování nabídky

7.1. Zadavatel požaduje, aby nabídka splňovala následující požadavky:

a) Nabídka musí být předložena v českém jazyce.
b) Nabídka nebude obsahovat přepisy a opravy, které by mohly zadavatele uvést v omyl.

7.2. Uchazeč zpracuje svou nabídku způsobem níže uvedeným:

a) Krycí list nabídky. Na krycím listu budou uvedeny zejména tyto údaje: název zakázky malého rozsahu, základní identifikační údaje zadavatele a uchazeče (včetně osob zmocněných k dalším jednáním), datum a podpis osoby oprávněné za uchazeče jednat (vzor krycího listu je přílohou č. 2).
b) Uchazeč jako součást nabídky předloží doklady prokazující jeho kvalifikaci:

• Uchazeč prokáže splnění profesních kvalifikačních předpokladů
  - výpisem z obchodního rejstříku, pokud je v něm zapsán, či výpisem z jiné obdobné evidence, pokud je v ní zapsán (ne starší než 90 kalendářních dnů od data vydání).
  - dokladem o oprávnění k podnikání v rozsahu odpovídajícím předmětu této zakázky, zejména doklad prokazující příslušné živnostenské oprávnění či licenci.

Doklady k prokázání splnění profesních kvalifikačních předpokladů lze předložit pouze v prosté kopii.

c) Cenovou nabídku (nabídková cena musí být zpracována v souladu s požadavky uvedenými v čl. 4 této zadávací dokumentace)
d) Technická specifikace a popis služby
e) Podepsaný návrh smlouvy (viz příloha č. 1)
f) Uchazeč předloží údaj, v jaké výši může poskytnout své služby k započtení náhradního plnění dle § 81 odst. 3 zákona č. 435/2004 Sb., o zaměstnanosti, v platném znění. Pokud uchazeč

takový údaj předloží, bude tento pro uchazeče závazný a bude jím taktéž zapracován v předloženém návrhu smlouvy.

g) Prohlášení, že uchazeč zachová mlčenlivost o všech skutečnostech, které nabyl na základě těchto zadávacích podmínek a takto nabyté údaje použije pouze pro zpracování nabídky do výběrového řízení k této zakázce. Prohlášení bude podepsané osobou oprávněnou jednat za uchazeče.
h) Prohlášení, že uchazeč bere na vědomí a souhlasí s tím, že zadavatel je povinen a zveřejní v souladu se zákonem č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, na základě žádosti veškerou zadávací dokumentaci k zakázce č. 120/14/OCN včetně smlouvy.
i) Nabídka bude podepsána osobou (-ami) oprávněnou (-nými) jednat za dodavatele.

8. Další požadavky zadavatele k průběhu výběrového řízení

Žádná osoba (dodavatel) se nesmí zúčastnit tohoto výběrového řízení jako uchazeč více než jednou.

V případě, že vznikne rozpor mezi údaji o zakázce obsaženými v různých částech zadávací dokumentace, jsou pro zpracování nabídky podstatné údaje obsažené v zadávací dokumentaci

Náklady uchazečů spojené s účastí ve výběrovém řízení zadavatel nehradí.

Zadavatel si nevyhrazuje právo požadovat úhradu nákladů souvisejících s poskytnutím zadávací dokumentace.

Pokud nabídka nebude úplná nebo v ní nebudou obsaženy veškeré doklady a informace stanovené touto zadávací dokumentací, vyhrazuje si zadavatel právo nabídku vyřadit.

Zadavatel si vyhrazuje právo před rozhodnutím o výběru nejvhodnější nabídky ověřit, případně vyjasnit informace deklarované uchazeči v nabídce.

Zadavatel si vyhrazuje právo vést toto výběrové řízení v souladu s pravidly stanovenými zejména v čl. 5 této zadávací dokumentace.

Zadavatel si vyhrazuje právo změny obsahu návrhu smlouvy, jenž je přílohou této zadávací dokumentace.

Zadavatel si vyhrazuje právo v rámci výběrového řízení jednat o všech částech nabídky uchazeče.

Jednání o nabídkách v rámci výběrového řízení je vedeno písemně prostřednictvím elektronické pošty. Zadavatel si vyhrazuje právo pozvat uchazeče k osobnímu jednání o nabídkách.

Komunikačním jazykem pro veškerá jednání v rámci výběrového řízení je stanovena čeština, nepřipustí-li zadavatel výslovně jinak.

Zadavatel si vyhrazuje právo kdykoliv v průběhu řízení toto řízení ukončit a zrušit bez udání důvodu, odmítnout všechny nabídky a neuzavřít smlouvu s žádným z uchazečů.

V souladu s ustanovením § 1740 odst. 3 poslední věta zákona č. 89/2012 Sb., občanský zákoník, v platném znění, platí, že předložení ze strany uchazeče podepsaného návrhu smlouvy s dodatkem nebo odchylkou proti požadavkům zadavatele nezakládá povinnost zadavatele takovou odchylku či dodatel akceptovat.

9. Výběrové řízení

9.1. Zahájení výběrového řízení

Výběrové řízení je zahájeno uveřejněním zadávací dokumentace na profilu zadavatele ČEPRO, a. s. na internetových stránkách www.softender.cz.

9.2. Dodatečné informace

Dodavatel je oprávněn požadovat písemně dodatečné informace k zadávacím podmínkám. Písemná žádost musí být zadavateli doručena nejpozději 5 dnů před uplynutím lhůty pro podání nabídek.

9.3. Místo, způsob a lhůta k podávání nabídek

Nabídka bude podána elektronicky do systému Softender (www.softender.cz), ve lhůtě nejpozději do 21. 10. 2014 do 10.00 hodin.

Nabídky lze podat v případě nutnosti i osobně nebo poštou na adresu sídla zadavatele, a to v pracovních dnech od 8.00 hod. do 14.00 hod. na podatelnu zadavatele. V případě písemného podání musí být nabídka podána v řádně uzavřené obálce, opatřené na přelepu razítkem a na přední straně označené „NEOTVÍRAT! VÝBĚROVÉ ŘÍZENÍ č. 184/14/OCN – „Analyzátor zranitelnosti“ ve výše uvedené lhůtě. Písemná nabídka musí obsahovat 1x originál nabídky v listinné podobě a podepsaný návrh smlouvy, 1x kompletní kopie nabídky v listinné podobě, 1x kompletní kopie nabídky v elektronické podobě (CD, DVD, flash-disk).

V případě zaslání nabídky poštou musí uchazeč zajistit, aby nabídka byla doručena zadavateli na uvedenou adresu sídla zadavatele nejpozději do výše uvedeného termínu.

9.4. Zadávací lhůta

Uchazeč je svou nabídkou vázán po dobu zadávací lhůty. Zadávací lhůta se stanovuje ve lhůtě 90 dnů ode dne skončení lhůty pro podání nabídek. Pro zadávací lhůtu platí v plném rozsahu ustanovení § 43 ZVZ.

10. Přílohy

Nedílnou součástí této zadávací dokumentace jsou její přílohy:
Příloha č. 1 – návrh smlouvy
Příloha č. 2 – vzor krycího listu nabídky

V Praze, dne 14. 10. 2014