VÝZVA K PODÁNÍ NABÍDKY

STAREZ – SPORT, a.s.

se sídlem Křídlovická 34, 603 00 Brno, IČO: 269 32 211

(dále jen „*zadavatel*“) tímto

v y z ý v á

k podání nabídky ve výběrovém řízení na veřejnou zakázku malého rozsahu na služby

Zajištění kybernetické bezpečnosti

(dále jen veřejná zakázka)

zadávanou mimo režim zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen zákon)

I. Preambule

1. Veškeré úkony v rámci výběrového řízení se provádějí elektronicky prostřednictvím elektronického nástroje E-ZAK dostupného na https://zakazky.starezsport.cz/ (nestanoví-li zadavatel v zadávacích podmínkách nebo v průběhu výběrového řízení jinak). Zadavatel dodavatele upozorňuje, že **pro plné využití všech možností elektronického nástroje E-ZAK je třeba provést a dokončit tzv. registraci dodavatele**. Vyřízení registrace trvá maximálně 48 hodin (v pracovní dny) a není zpoplatněno.
2. Zadavatel dodavatelům doporučuje, aby kontaktní osobu zadavatele požádali o přiřazení k veřejné zakázce nebo aby průběžně sledovali adresu veřejné zakázky.
3. Zavedl-li zadavatel dodavatele do elektronického nástroje E-ZAK, uvede u něj jako kontaktní údaje takové, které získal jako veřejně přístupné, nebo jiné vhodné kontaktní údaje. Je povinností každého dodavatele, aby před dokončením registrace do elektronického nástroje E-ZAK své kontaktní údaje zkontroloval a případně upravil či doplnil jiné.
4. Veškeré písemnosti zasílané prostřednictvím elektronického nástroje E-ZAK se považují za řádně doručené dnem jejich doručení do uživatelského účtu adresáta písemnosti v elektronickém nástroji E-ZAK. Na doručení písemnosti nemá vliv, zda byla písemnost jejím adresátem přečtena, případně, zda elektronický nástroj E-ZAK adresátovi odeslal na kontaktní emailovou adresu upozornění o tom, že na jeho uživatelský účet v elektronickém nástroji E-ZAK byla doručena nová zpráva, či nikoli.
5. Podrobné informace o ovládání systému naleznete v uživatelské příručce dostupné na: https://zakazky.starezsport.cz/
6. Zadavatel má zájem, s ohledem na povahu a smysl této veřejné zakázky, dodržovat zásady sociálně odpovědného zadávání, environmentálně odpovědného zadávání a inovací ve smyslu zákona, přičemž dodavatel je povinen tyto zásady dodržovat. Sociálně odpovědné zadávání kromě důrazu na čistě ekonomické parametry zohledňuje také související dopady zejména v oblasti zaměstnanosti, sociálních a pracovních práv a životního prostředí. Zadavatel od dodavatele vyžaduje při plnění předmětu veřejné zakázky zajistit zejména legální zaměstnávání, férové pracovní podmínky a odpovídající úroveň bezpečnosti práce pro všechny osoby, které se na plnění veřejné zakázky budou podílet. Dodavatel je povinen zajistit tento požadavek zadavatele i u svých poddodavatelů.

II. Předmět veřejné zakázky

Předmětem veřejné zakázky je zajištění služeb v oblasti kybernetické bezpečnosti podle vymezených technických podmínek (specifikace). Konkrétně se bude jednat o služby v oblasti penetračního testování a skenování zranitelností.

Služby budou poskytovány pravidelně v rozmezí dvou let a budou zahrnovat dodávku služeb penetračního testování a skenování zranitelností v minimálním rozsahu:

Penetrační testování: 1x ročně

Skenování zranitelností: 4x ročně

a) **Penetrační testování Externí**

Počet webových prezentací s minimem dynamických funkcí: 20

Počet IP/ rozsah: 12

Zadavatel požaduje v rámci Externích penetračních testů provedení exploitace alespoň jedné definované zranitelnosti.

b) **Penetrační testování Interní**

Testování bude zahrnovat celou interní infrastrukturu společnosti.

Interní penetrační test bude neautentizovaný (přístup k síťové zásuvce) a autentizovaný (přístup k oprávněním běžného uživatele).

Interní penetrační test bude realizován v jedné lokalitě objednatele **Brno** a bude zahrnovat minimálně následující infrastrukturu:

Počet stanic: 193

Počet serverů (fyzických i virtualizovaných): 50

Počet síťových zařízení: 85

Systém řízení chemie: 5

Zabezpečovací systém: 6

c) **Penetrační testování WiFi sítí**

Testování bude provedeno ve stejné lokalitě jako Interní penetrační testování

Počet přístupových bodů (AP): 65

Počet přístupových segmentů (SSID): 5

Bude zahrnovat minimálně následující techniky:

- Ověření bezpečné konfigurace (metody autentizace, kryptografie)
- Ověření segregace segmentů sítě
- Odposlouchávání přihlašovacích údajů a jejich bruteforce cracking
- „Útok zlého dvojčete" ("Evil Twin")

d) **Penetrační testování Webových aplikací**

Počet webových aplikací	5
Počet dynamických funkcí (vyhledávání, odeslaní dotazníku, přihlašování)	6

e) **Skenování zranitelností**

- Skenování zranitelností musí být prováděno minimálně **1x kvartálně**
- Výsledky skenování musí být předávány srozumitelnou formou v interaktivním dashboardu, který musí zahrnovat minimálně následující informace:
  - Počet zranitelnosti a jejich rozdělení podle závažnosti
  - Počet skenovaných zařízení/technologií/asetů
  - Počet zranitelných asetů danou zranitelností
  - Počet patchovatelných a nepatchovatelných zranitelností
  - Seznam nejběžnějších zranitelností v prostředí (zranitelnost na největším počtu zařízení)
  - Seznam Nejkritičtějších zranitelností (kategorie 5 nebo 4)
  - Seznam nejzranitelnějších zařízení (zařízení s největším počtem zranitelností)
  - Možnosti filtrace podle
    - Závažnosti / severity ve škále 1-5 (1 nejméně závažné, 5 kritické)
    - Typu nebo kategorie zranitelností (Windows, Linux, Security)
    - Patchovatelné/nePatchovatelné zranitelnosti
    - Vendora
  - Každá zranitelnost musí poskytovat
    - detailní informace popisující danou zranitelnost
    - popis dopadů zranitelnosti
    - řešení zranitelnosti včetně přímých odkazů na dodatečné zdroje a řešení.
- Rozsah prostředí bude pro odhad rozsahu
  - Počet zařízení: 259

Po každém provedeném testování zhotovitel zpracuje závěrečnou zprávu z penetračního testu v rozsahu minimálně:

1) Cíl a rozsah projektu. Popis předmětu projektu.
2) Popis testovacího scénáře a popis jednotlivých metodik, použité nástroje. Zdůvodnění postupů a použitých nástrojů.
3) Stanovení stupnice a metodiky hodnocení (nejméně dle metodiky zadavatele, CVE, CVSS). Kategorizace zjištěných zranitelností a jejich přehledné značení.
4) Detailní postup provedených testů včetně použitých nástrojů a technik použitých v jednotlivých fázích.
5) Popis zjištění/nálezů (pro účely VŘ smyšlených) z jednotlivých fází testů.
6) Popis nalezených zranitelností a možností jejich zneužití.
7) Doporučení pro odstranění identifikovaných slabin a zranitelných míst.

8) Manažerské shrnutí.

Předmět veřejné zakázky je dále specifikován touto výzvou (některé povinné požadavky jsou např. promítnuty do popisu hodnocení) a jejími přílohami, které obsahují požadavky zadavatele na plnění veřejné zakázky. Tyto požadavky je dodavatel povinen respektovat. Nebude-li nabídka splňovat zadávací podmínky, může ji zadavatel z výběrového řízení vyloučit. Příkladem nesplnění zadávacích podmínek je chybějící část zprávy nebo část zprávy, která nebude odpovídat požadavkům zadavatele (např. v kapitole doporučení pro odstranění nebudou obsažena žádná doporučení).

III. Předpokládaná doba plnění

Smlouva bude uzavřena na období dvou let.

IV. Místo plnění a prohlídka místa plnění

Služba je poskytována vzdáleným přístupem na serverech STAREZ – SPORT, a.s.

V. Lhůta pro podání nabídky

Lhůta pro podání nabídek: **do 29. 9. 2023 do 12.00 hodin.**

VI. Místo pro podání nabídky

Nabídky se podávají prostřednictvím elektronického nástroje na adrese veřejné zakázky.

VII. Požadavky zadavatele na kvalifikaci

Dodavatelé jsou povinni prokázat kvalifikaci požadovanou zadavatelem. Požadavky na kvalifikaci jsou zadavatelem stanoveny ve formuláři nabídky. Dodavatel, který nesplní kvalifikaci požadovaným způsobem a v požadovaném rozsahu, může být zadavatelem z účasti ve výběrovém řízení vyloučen.

VIII. Závaznost obecných zadávacích podmínek a vysvětlení, změna nebo doplnění zadávací dokumentace

a) Závaznost požadavků zadavatele

Informace a údaje uvedené v této výzvě vymezují závazné požadavky zadavatele na plnění veřejné zakázky. Dodavatel, který nesplní stanovené požadavky zadavatele, může být zadavatelem z účasti ve výběrovém řízení vyloučen.

b) Vysvětlení, změna nebo doplnění zadávací dokumentace

Žádost o vysvětlení může účastník zasílat zadavateli elektronicky prostřednictvím elektronického nástroje. Zadavatel je oprávněn uveřejnit na profilu zadavatele vysvětlení zadávací dokumentace i z vlastního podnětu. Takto může rovněž uveřejnit změnu nebo doplnění zadávací dokumentace. Pokud to povaha doplnění nebo změny zadávací dokumentace vyžaduje, zadavatel současně přiměřeně prodlouží lhůtu pro podání nabídek.

IX. Obsah nabídky

Zadavatel přílohou zadávací dokumentace předkládá dodavatelům vzorový **formulář nabídky** obsahující požadavky zadavatele, kterými je podmiňována účast dodavatelů ve výběrovém řízení.

Splnění veškerých požadavků zadavatele, tj. požadavků na předmět veřejné zakázky, na kvalifikaci nebo na předložení údajů rozhodných pro hodnocení, prokáží dodavatelé předložením formuláře nabídky včetně příslušných příloh nebo jiných rovnocenných dokladů.

Zadavatel stanovuje, že nabídka uchazeče musí obsahovat tyto dokumenty:

a) formulář nabídky

b) závěrečná zpráva z penetračního testu a ukázka vulnerability dashboardu

c) kvalifikační doklady a seznam členů týmu

Návrh smlouvy ani ostatní dokumenty nemusí být do nabídky přikládány.

V případě rozporu mezi celkovou nabídkovou cenou zapsanou ve formuláři nabídky a mezi celkovou nabídkovou cenou uvedenou jinde v textu nabídky nebo jejích přílohách, budou pro účely hodnocení nabídek a realizaci plnění použity údaje uvedené ve formuláři nabídky.

X. Způsob výběru nejvhodnější nabídky (hodnocení nabídek)

Hodnocení nabídek bude provedeno podle základního hodnotícího kritéria ekonomická výhodnost nabídky, a to dle následujících dílčích hodnotících kritérií:

Hodnotící kritérium	váha
A) Nabídková cena	*80 %*
B) Kvalita vzorové závěrečné zprávy z penetračního testu a ukázka vulnerability dashboardu	*20 %*

Hodnoceny budou údaje uvedeny ve formuláři nabídky.

V rámci kritéria hodnocení A Nabídková cena bude zadavatel hodnotit celkovou cenu za jeden měsíc poskytování služeb (měsíční paušál).

Nabídková cena bude stanovena jako cena nejvýše přípustná a platná po celou dobu realizace veřejné zakázky. Nabídková cena bude obsahovat veškeré náklady dodavatele nezbytné pro řádnou a včasnou realizaci předmětu veřejné zakázky včetně nákladů souvisejících (např. poplatky, vedlejší náklady, kurzovní rizika, předpokládaná rizika spojená s realizací předmětu plnění veřejné zakázky, příp. cestovní náklady apod.).

V rámci kritéria hodnocení B Kvalita vzorové zprávy bude zadavatel hodnotit kvalitu závěrečné zprávy z penetračního testu a ukázku vulnerability dashboardu.

Do popisu hodnocení se promítají i povinné požadavky na obsah a rozsah zprávy.

- Vzorová závěrečná zpráva musí být zpracována v takovém rozsahu a obsahu v jakém budou zpracovávány závěrečné zprávy pro plnění v rámci veřejné zakázky.

- Minimální rozsah závěrečné zprávy:
    1) Cíl a rozsah projektu. Popis předmětu projektu.
    2) Popis testovacího scénáře a popis jednotlivých metodik, použité nástroje. Zdůvodnění postupů a použitých nástrojů.
    3) Stanovení stupnice a metodiky hodnocení (nejméně dle metodiky zadavatele, CVE, CVSS). Kategorizace zjištěných zranitelností a jejich přehledné značení.
    4) Detailní postup provedených testů včetně použitých nástrojů a technik použitých v jednotlivých fázích.
    5) Popis zjištění/nálezů (pro účely VR smyšlených) z jednotlivých fází testů.
    6) Popis nalezených zranitelnosti a možností jejich zneužití.
    7) Doporučení pro odstranění identifikovaných slabin a zranitelných míst.
    8) Manažerské shrnutí.

Zpráva bude hodnocena po jednotlivých částech (aspektech) dle níže uvedeného (u částí jsou maximálními body uvedeny váhy jejich důležitosti):

Ad 1) Cíl a rozsah projektu. Popis předmětu projektu

Popis testovaného objektu/projektu/aplikace/infrastruktury.

Zadavatel očekává/bude pozitivně hodnotit: jasnou definici cíle testování a pravděpodobných zranitelností a z toho vyplývajících rizik. Z popisu musí být pochopitelný a zdůvodnitelný zvolený rozsah testování. Zadavatel jednotlivým nabídkám přidělí v rámci daného kritéria bodovou hodnotu max. 5 bodů.

Ad 2) Popis testovacího scénáře a popis jednotlivých metodik, standardů, použitých nástrojů

Aby zadavatel mohl posoudit vhodnost a relevantnost použitých testů, je nezbytné relevantním způsobem popsat testovací scénář a jednotlivé použité metodiky a standardy. Z této části musí být zjevná opodstatněnost provedeného testu, jeho rozsah a vhodnost použitých SW produktů/nástrojů.

Zadavatel očekává/bude pozitivně hodnotit: Hodnocení bude provedeno z pohledu pochopitelnosti, přesnosti a podrobnosti, tak aby byl jednoznačně vymezen důvod použitého testu jeho vhodnost a úplnost a zda splňuje svým zaměřením požadavky na testovaní. Smyslem je posoudit vhodnost navržených a prováděných testů. Dále bude hodnocena kvalita popsaného testovacího scénáře, tak aby bylo možné vyhodnotit provedené testy a zejména následné získání dalších podkladů pro postup při odstraňování nedostatků a slabých míst testovaného systému. Pro vhodné posouzení je nezbytné také popsat dále použité metody hodnocení pro klasifikaci identifikovaných nálezů (pokud jsou použity jiné než požadované zadavatelem). Zadavatel jednotlivým nabídkám přidělí v rámci daného kritéria bodovou hodnotu max. 15 bodů.

Ad 3) Detailní postup provádění navržených testů včetně použitých nástrojů a technik použitých v jednotlivých fázích.

V rámci této kapitoly, zadavatel vyžaduje popis použitých SW produktů/nástrojů a technik v rámci jednotlivých skupin testů, aby mohl vyhodnotit opodstatněnost provedených testů, aby mohl vhodně posoudit kvalitu a rozsah provedených testů a přijmout vhodná opatření pro odstranění identifikovaných zranitelností/chyb/nedostatků.

Zadavatel očekává/bude pozitivně hodnotit: co největší rozsah (detailnost) a použitelnost popisu relevantních okolností pro odstranění nálezů a opodstatněnost a rozsah provedených testů a nástrojů při zachování co největší srozumitelnosti (efektivity) popisu. Zadavatel jednotlivým nabídkám přidělí v rámci daného kritéria bodovou hodnotu max. 10 bodů.

Ad 4) Stanovení stupnice a metodiky. Kategorizace zjištěných zranitelností a jejich přehledné značení.

Bude hodnocen provedený popis identifikovaných zranitelností a s tím související metodika, kategorizace a značení zranitelností.

Zadavatel očekává/bude pozitivně hodnotit: detailnější popis zranitelností při zachování dostatečné efektivity popisu, zejména bude považováno za kladné, že popisy zranitelností obsahují jednoznačný identifikátor, detailní popis a skóre, kterého jednotlivé zranitelnosti dosáhly a samotné skóre zranitelnosti.

Pozitivně zohledněno bude také použití mezinárodních standardů při hodnocení. Zadavatel požaduje provedení hodnocení dle standardů CVE, CVSS, případně i dle dalších standardů. Významným aspektem při hodnocení je provedení kategorizace identifikovaných nálezů/zjištění, aby byl splněn účel zprávy. Zadavatel bude hodnotit relevantnost ve zprávě poskytnutých hodnocení, neboť dle hodnocení bude dále postupovat při prioritizaci odstraňování nálezů. Při použití dalších metodik hodnocení je nezbytné identifikovat dané metodiky, popsat a provést hodnocení daného nálezu. Více způsobu hodnocení zadavatel preferuje, neboť může vést k přesnější identifikaci daného nálezu. Zadavatel jednotlivým nabídkám přidělí v rámci daného kritéria bodovou hodnotu max. 5 bodů.

Ad 5) Popis zjištění/nálezů (pro účely VR smyšlených) z jednotlivých fází testů. Hodnocení předloženého důkazu.

V rámci kapitoly bude hodnocen popis identifikovaných nálezů/zranitelností v rámci jednotlivých fází testů. Zohledněna bude také kvalita popisu, a to jak technického, tak manažerského ke každé zranitelnosti/nálezu.

Zadavatel očekává/bude pozitivně hodnotit: podrobnost a přesnost popisu, hodnocení zranitelnosti/nálezu. Výše uvedené bude posuzováno z pohledu jeho použitelnosti pro odstranění daného nálezu/zranitelnosti. Velký důraz bude kladen na předložený důkaz o identifikovatelném nálezu/zranitelnosti. Důkaz a jeho průkaznost bude hodnocen vzhledem k provedenému testu, zejména s ohledem na průkaznost tohoto důkazu o provedeném testu, jeho rozsahu a kvality provedeného testování. Zadavatel jednotlivým nabídkám přidělí v rámci daného kritéria bodovou hodnotu max. 25 bodů.

Ad 6) Popis nalezených zranitelnosti a možností jejich zneužití

Bude hodnocen provedený popis možných využití k daným nálezům/zranitelnostem.

Zadavatel očekává/bude pozitivně hodnotit: využitelnost při následném získání dalších podkladů pro postup při odstraňování nedostatků a slabých míst způsobených danou zranitelností. Významným aspektem je relevance popsaných možností zneužití. Zadavatel jednotlivým nabídkám přidělí v rámci daného kritéria bodovou hodnotu max. 15 bodů.

Ad 7) Doporučení pro odstranění identifikovaných slabin a zranitelných míst.

Zadavatel očekává/bude pozitivně hodnotit: co největší rozsah a nejvyšší kvalitu popisu možných způsobů odstranění u identifikovaných zranitelností. Zejména s pohledem k získání poučení a informací vedoucích k odstranění identifikované zranitelnosti. Zadavatel jednotlivým nabídkám přidělí v rámci daného kritéria bodovou hodnotu max. 15 bodů.

Ad 8) Manažerské shrnutí

Shrnutí závěrů testu pro management, přičemž toto shrnutí musí obsahovat rovněž závěrečné zhodnocení provedeného testu a hodnocení aktuálně dosažené úrovně bezpečnosti testovaných aplikací.

Zadavatel očekává/bude pozitivně hodnotit: takové manažerské shrnutí, které bude určené pro rychlé zorientování se všech zainteresovaných subjektů (viz výše) v identifikovaných nálezech a celkovém hodnocení testovaného objektu. Přihlížet se bude také k uživatelské přívětivosti a přehlednosti ukázky vulnerability dashboardu (přívětivější a přehlednější bude hodnocena lépe). Zadavatel jednotlivým nabídkám přidělí v rámci daného kritéria bodovou hodnotu max. 15 bodů.

Způsob hodnocení nabídek:

Hodnocení nabídek v jednotlivých kritériích hodnocení bude provedeno bodovací metodou založenou na stobodové stupnici. Každé jednotlivé nabídce bude dle dílčího kritéria přidělena bodová hodnota, která odráží úspěšnost nabídky v rámci dílčího kritéria.

Zadavatel bude lépe hodnotit jednotlivé části i s ohledem na jejich vzájemnou provázanost, ucelenost a celkovou komplexnost zprávy.

V případě hodnotícího **kritéria A. (nabídková cena)** se jedná o kvantitativní kritérium, u něhož jsou preferovány nižší hodnoty před vyššími; jednotlivým nabídkám dle uvedeného kritéria budou přiděleny bodové hodnoty dle následujícího vzorce:

$$\text{Počet bodů} = \frac{\text{nabídka s nejnižší hodnotou (nejnižší cenou)}}{\text{hodnocená nabídka}} \times 100$$

V případě **hodnotícího kritéria B. (kvalita vzorové zprávy)** se jedná o kvantitativní kritérium, u něhož jsou preferovány vyšší hodnoty před nižšími.

V rámci tohoto kritéria bude hodnocena kvalita závěrečné zprávy z penetračního testu a ukázka vulnerability dashboardu. Zpráva bude hodnocena po jednotlivých částech, přičemž za každou splněnou část je možné obdržet maximální počet bodů uvedený výše, pokud zpráva v dané části maximálně naplní shora vymezené požadavky zadavatele. Celkem může účastník získat sto bodů. Následně budou přidělené body sečteny a jednotlivým nabídkám dle uvedeného kritéria budou přiděleny bodové hodnoty dle následujícího vzorce:

$$\text{Počet bodů} = \frac{\text{hodnocená nabídka}}{\text{nabídka s nejvyšší hodnotou (největším počtem bodů)}} \times 100$$

CELKOVÉ BODOVÉ HODNOCENÍ NABÍDKY bude sestaveno na základě součtu příslušnými vahami převážených bodových hodnot dosažených v jednotlivých dílčích kritériích. Výsledné pořadí úspěšnosti jednotlivých nabídek bude stanoveno tak, že za nejvhodnější bude považována nabídka, která dosáhla nejvyšší hodnoty součtu převážených bodových hodnot v rámci všech dílčích hodnotících kritérií.

XI. Kontaktní osoba zadavatele

Kontaktní osobou zadavatele ve věcech souvisejících s tímto výběrovým řízením je

Mgr. David Zuska, tel. +420 737 566 827, email: zuska@starezsport.cz nebo Mgr. Rostislav Gnida, tel. +420 734 690 922, email: gnida@starezsport.cz.

XII. Závěrečná ustanovení

Účastník výběrového řízení nemá nárok na úhradu nákladů souvisejících s účastí ve výběrovém řízení (např. nákladů na zpracování nabídky).

Zadavatel je oprávněn ověřovat údaje uvedené účastníkem výběrového řízení v nabídce. V případě, že zadavatel zjistí, že informace uvedené v nabídce účastníka nejsou pravdivé, je zadavatel oprávněn takového účastníka vyloučit z další účasti ve výběrovém řízení.

Zadavatel je oprávněn požadovat po účastníkovi objasnění nebo doplnění nabídky. V případě, že účastník na výzvu zadavatele nabídku neobjasní nebo nedoplní, je zadavatel oprávněn vyloučit účastníka z další účasti ve výběrovém řízení.

Zadavatel si vyhrazuje právo výběrové řízení zrušit bez udání důvodu.

Zadavatel jako správce osobních údajů informuje subjekty údajů, od nichž obdrží nabídku, že osobní údaje zpracovává výhradně z důvodu a za účelem splnění právních povinností stanovených zákonem č. 134/2016 Sb., o zadávání veřejných zakázek.

Přílohy

A. Formulář nabídky

B. Obchodní podmínky

V Brně dne 14. 9. 2023

Mgr. Martin Mikš, generální ředitel

STAREZ – SPORT, a.s.