Pozvánka na veřejnou diskuzi za účelem průzkumu trhu

(předběžné tržní konzultace pro optimální nastavení podmínek veřejné soutěže)

Účel a termín předběžných konzultací

Zadavatel plánuje **realizovat veřejnou soutěž s cílem poskytování služeb zajištění role manažera kybernetické bezpečnosti** pro Univerzitu Hradec Králové (též jen „UHK"). Za tímto účelem je zadavatel připraven představit svůj záměr prostřednictvím těchto veřejných předběžných konzultací pro potenciální poskytovatele této služby.

Cílem UHK v rámci předběžných tržních konzultací (dále též jen i „PTK") je získat informace z trhu, které pomohou vymezit předmět a podmínky realizace veřejné zakázky tak, aby podmínky soutěže co nejlépe odpovídaly jeho potřebám a aby byly stanoveny v souladu s praktickými souvislostmi vycházející z reálné možnosti trhu.

Záměrem Zadavatele je využití a získání zdrojů, know-how a organizačních zkušeností poskytovatelů v provádění odborných expertních a poradenských činností na zajištění výkonu činnosti manažera kybernetické bezpečnosti (dále též jen „KB") pro UHK, a to v souladu s:

- se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů ve znění pozdějších předpisů (dále jen „zákon o kybernetické bezpečnosti")
- vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, v platném znění (dále jen „vyhláška o kybernetické bezpečnosti)
- vyhláškou č. 360/2020 Sb., na základě které došlo k novele vyhlášky č. 317/2014 Sb., o významných informačních systémech (VIS) a jejich určujících kritériích, která je určující pro orgány veřejné moci.

Tyto konzultace se budou **konat** dne **17. 03. 2022**, v zasedací místnosti rektorátu UHK **–** na **adrese Rokitanského 62, Hradec Králové.**

Tyto PTK budou **individuální**, vedené s každým zájemcem o PTK v časovém **rozsahu cca 30 minut**.

Vaši účast potvrďte prosím na zakazky@uhk.cz do 15. 03 2022 – bude s Vámi dohodnut konkrétní čas vaší účasti.

Na tyto PTK si prosím připravte **stručný přehled o vaší společnosti** (max. 2 slidy) **a** máte-li zkušenosti s realizací **role Manažera KB, pak i přehled o vašich zkušenostech s touto rolí** (max. 5 slidů).

Zadavatel upozorňuje, že těchto PTK bude pořizovat audiozáznam.

Konkrétní návrhy k diskusi na těchto konzultacích

V rámci předběžných konzultací Zadavatel očekává, že v rámci osobní předběžné kolektivní konzultace (průzkumu trhu) získá odpovědi na následující okruhy témat:

1/ Předpokládané minimální požadavky na kvalifikaci a způsobilost plánované soutěže na zajištění role manažera kybernetické bezpečnosti:

i/ V rámci technické kvalifikace UHK předpokládá zohlednění 2 poskytnutých min. ročních služeb v pozici manažera KB v minulých 5 letech – je toto reálné?

ii/ V rámci podmínek pro manažera KB/ poskytovatele je předložení získané Certifikace – alespoň jednu z níže uvedených – je toto dostatečné?:

a) Certified Information Security Manager (CISM),

b) Certified in Risk and Information Systems Control (CRISC),

c) Certified Information Systems Security Proffessional (CISPP),

d) Manažer BI (akreditační schéma ČIA).

2/ Reálnost/splnitelnost požadavků – viz příloha níže.

3/ Určení minimálního rozsahu podaných informací pro seznámení s kontextem organizace.

4/ Určení optimální délky a podmínek smluvního vztahu – s ohledem na ekonomický dopad pro UHK.

5/ Specifikace dalších potřeb dodavatelů od zadavatele pro přípravu kvalitní nabídky.

6/ Odhad předpokládané časové náročnosti služby. Paušální sazba za měsíc X sazba na hodinu?

7/ Určení finančního rámce pro naplnění požadavků objednatele a optimalizace smluvních plateb za definované služby.

8/ Hodnocení na nejnižší nabídkovou cenu X hodnocení na kvalitu – cena + zkušenosti Manažera KB.

9/ Plán UHK: nebude se povolovat plnění přes poddodavatele.

10/ Předpokládané náklady na službu v jednotlivých letech.

11/ Reálnost předpokladu zahájení spolupráce: květen 2022?

Příloha PTK : Základní informace pro předmět plnění plánované soutěže

Poskytovatel bude poskytovat pro Objednatele následující služby zahrnující následující plnění:

- Zajištění úkonů vyplývajících z povinností role manažera kybernetické bezpečnosti, a to v souladu se všemi výše uvedenými právními předpisy (převzetí této role v organizaci UHK).
- Odpovědnost za řízení a prosazování systému řízení bezpečnosti informací.

- Informování vedení organizace (popř. osob pověřených UHK k agendě kybernetické bezpečnosti) o aktuálním stavu systému řízení bezpečnosti informací.
- Tvorba, prosazování a zajišťování aktualizace Bezpečnostní politiky informací v rámci UHK.
- Tvorba, prosazování a zajišťování aktualizace dokumentace Systému řízení bezpečnosti informací dle požadavků zákona o kybernetické bezpečnosti a jeho prováděcích vyhlášek pro UHK.
- Kontrola dodržování Systému řízení bezpečnosti dle požadavků zákona o kybernetické bezpečnosti a jeho prováděcích vyhlášek.
- Spolupráce při optimalizaci organizačního uspořádání informační a kybernetické bezpečnosti a návrhu budoucího modelu řízení informační a kybernetické bezpečnosti.
- Spolupráce při vytváření standardů informační a kybernetické bezpečnosti, konceptů plánů obnovy a dalších pravidel, včetně standardizace procesů informační a kybernetické bezpečnosti.
- Spolupráce při harmonizaci a optimalizaci nastavení procesů a činností informační a kybernetické bezpečnosti.
- Spolupráce při identifikaci aktuálního rozsahu a úplnosti informací o aktivech, identifikaci zdrojů, a návrhu na způsoby doplnění chybějících informací (information asset management).
- Spolupráce při procesu řízení rizik, jejich rozsahu a dopadu.
- Spolupráce při vytvoření katalogu služeb pro oblast informační a kybernetické bezpečnosti, tvorbě norem a standardů (SLA a KPI) v souladu s platnými právními předpisy a technickými normami.
- Podpora implementace nových procesů a zajištění přechodu na nové modely fungování informační a kybernetické bezpečnosti.
- Koordinace opatření ke zvýšení bezpečnostního povědomí v organizaci a školení zaměstnanců organizace v oblasti kybernetické bezpečnosti.
- Dohled nad Provozovateli a Významnými dodavateli z pohledu plnění požadavků zákona o kybernetické bezpečnosti a prováděcích předpisů – pravidelné informování a aktuálním stavu.
- Ověřování a vyšetřování kybernetických bezpečnostních incidentů, včetně zvládání kybernetických bezpečnostních událostí, a informování Výboru pro řízení kybernetické bezpečnosti statutárního města Brna o bezpečnostních incidentech, zjištěných neshodách a nedostatečné efektivnosti bezpečnostních opatření.
- Příprava podkladů pro realizaci bezpečnostních opatření (organizační a technická).
- Vyhodnocování vhodnosti a účinnosti bezpečnostních opatření.
- Spolupráce při auditech kybernetické bezpečnosti a jejich analýze.
- Vystupování jménem organizace k regulačním orgánům v oboru informační a kybernetické bezpečnosti.
- Příprava a personalizace kurzu kybernetické bezpečnosti v LMS systémech objednatele a provádění školení z oblasti bezpečnosti informačních technologií.
- Zajištění zastupitelnosti bezpečnostní role manažera kybernetické bezpečnosti.

Poskytovatel služby zajištění role Manažera KB bude zodpovídat za plánování, organizování a řízení realizace opatření, projektů a programů k řízení bezpečnosti informací tak, aby bylo dosaženo cílů stanovených zákonem o kybernetické bezpečnosti a jeho prováděcími předpisy, a to ve stanoveném termínu a v rámci stanoveného rozpočtu.
Zajištění služby role Manažera KB působí jako „kontaktní" osoba pro veškeré aspekty a otázky kybernetické bezpečnosti a prosazuje a koordinuje úlohu systému řízení informační bezpečnosti v organizaci. Při výkonu svojí funkce se řídí pokyny rektora a výboru kybernetické bezpečnosti.

Univerzita Hradec Králové

Pravomoci a odpovědnosti role

Manažer KB je osoba odpovědná za systém řízení bezpečnosti informací od prevence až po eliminaci následků a vyhodnocení „úspěšných" kybernetických incidentů. Odpovídá za tvorbu a aktualizaci Strategie kybernetické bezpečnosti a Bezpečnostní politiky informací. Manažer KB je výkonným protějškem NÚKIB pro případy řešení kritických kybernetických bezpečnostních událostí.

Předpokládané požadované klíčové činnosti:

- Účast na jednáních Výboru pro řízení kybernetické bezpečností UHK.
- Odpovědnost za řízení systému řízení bezpečnosti informací.
- Pravidelný reporting pro vrcholové vedení Objednatele.
- Pravidelná komunikace s vrcholovým vedením Objednatele.
- Předkládání Zpráv o hodnocení aktiv a rizik, Plánu zvládání rizik a Prohlášení o aplikovatelnosti výboru pro řízení kybernetické bezpečnosti.
- Poskytování pokynů pro zajištění bezpečnosti informací při vytváření, hodnocení, výběru, řízení a ukončení dodavatelských vztahů v oblasti ICT.
- Komunikace s GovCERT/CSIRT.
- Podílení se na procesu řízení rizik.
- Koordinace řízení incidentů.
- Vyhodnocování vhodnosti a účinnosti bezpečnostních opatření.
- Příprava a personalizace kurzu kybernetické bezpečnosti v LMS systémech objednatele a provádění školení z oblasti

JUDr. Šárka Karlová

Digitálně podepsal JUDr. Šárka Karlová
Datum: 2022.03.08 10:36:09 +01'00'