Název zadavatele: Karlovarský kraj
Sídlo: Závodní 353/88
360 06 Karlovy Vary
IČO: 70891168
Vyřizuje: Bc. Monika Ille Toušová
Č. j.: KK/1345/OP/25

Vysvětlení zadávací dokumentace č. 3

v souladu s ust. § 98 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“)

veřejné zakázky:**„Provedení penetračních testů se zaměřením na bezpečnost informačních systémů Krajského úřadu Karlovarského kraje a Provedení auditu kybernetické bezpečnosti“**

identifikátor zakázky (systémové číslo VZ): **„P25V00001031“**

Dne 16. 10. 2025 obdržel zadavatel výše uvedené veřejné zakázky prostřednictvím elektronického nástroje E-ZAK žádosti o vysvětlení zadávací dokumentace.

Zadavatel připravil vysvětlení formou otázek a odpovědí:

Dotaz č. 1

Může zadavatel vysvětlit, proč se povinnost mlčenlivosti nevztahuje i na něj; případně upraví předmětné ustanovení tak, aby platilo pro obě strany stejně?

Odpověď:
Zadavatel v návrhu smlouvy o poskytování služeb (příloha č. 2 zadávací dokumentace) upravil ustanovení článku IV. Mlčenlivost.

Dotaz č. 2

Může zadavatel upřesnit, zda počítá s rizikem vzniku takové újmy v důsledku řádně provedeného testování a zda bude ve smlouvě výslovně upravena odpovědnost dodavatele – zejména její vyloučení nebo omezení v případech, kdy újma nevznikla úmyslně nebo z hrubé nedbalosti?

Odpověď:
Zadavatel nepočítá s rizikem vzniku újmy. Zadavatel v návrhu smlouvy o poskytování služby doplnil ustanovení č. I Předmět smlouvy:
1.7. Poskytovatel odpovídá za škodu způsobenou porušením smlouvy nebo nedbalým či úmyslně chybným postupem. Pokud k dopadu (ohrožení, omezení či nefunkčnost testovaných informačních systémů) dojde i při dodržení doporučených standardů pro provádění penetračních testů, jako je např. metodika OSSTMM a standardy NIST 800-11 a další a dohodnutých limitů, odpovědnost nebude na straně poskytovatele těchto testů.

Dotaz č. 3

Zároveň může zadavatel také sdělit, zda bude možné smluvně upravit výčet rizik spojených s testováním (např. formou přílohy smlouvy) a zda bude možné předem stanovit maximální výši pojistného plnění odpovědnosti dodavatele

Odpověď:
Výčet rizik nebude smluvně upraven, protože nikdy nelze uvést 100 % výčet možných rizik. Max. výše pojistného plnění není stanovena.

Dotaz č. 4

Upraví tedy zadavatel Smlouvu tak, že doplní limitaci výše škody, kterou bude oprávněn na dodavateli požadovat?

Odpověď:
Článek V. smlouvy byl částečně upraven v rámci předchozího dotazu jiné společnosti, ale max. výše pojistného plnění nebyla stanovena a odst. o právu na náhradu škody v plné výši zůstal zachován. Limit max. výše škody nelze v tomto případě plně odhadnout, protože nikdo neví, jaké škody mohou nastat, v případě např. nenadálé nedostupnosti některých informačních systémů apod. Z tohoto důvodu nejsou možná rizika zahrnuta ve smlouvě, neboť není možné uvést jejich úplný (stoprocentní) výčet.

Dotaz č. 5

Účastník žádá zadavatele o upřesnění následujících dotazů pro nacenění technické části nabídky:

a) Obecné Požadujete retesty po nápravě zranitelností?

Odpověď: ANO

b) Externí penetrační test

- Rozsah - počet externě dostupných systémů, webových aplikací / URL, které mají být testovány (alespoň hrubý odhad).

Odpověď: Cca 10 URL

- Potvrzení, že test má být proveden jako nekooperativní (black-box), jak je v zadání, a pouze v případě, že obsahuje chybu/zranitelnost preferujete částečný gray-box přístup? Můžete uvést příklad?

Odpověď: Test dle zadání, ANO, příklady se neuvádí

- Potvrzení, že kontrola e-mailové infrastruktury z webů objednatele (např. test formulářů) umožní dodavateli spustit testy (odeslat email) a také ověřit informace v hlavičkách (přijmout email)?

Odpověď: ANO

- Pro test účinnosti antispamu bude k dispozici emailový účet s cílem validovat výsledky provedených testů?

Odpověď: ANO, bude k dispozici e-mailový účet

- Popište cíle testu "spolehlivost konfigurace" pro externí testy.

Odpověď: Ověření, že systémy jsou správně nastaveny a neobsahují chyby, které by mohly být zneužity. Testování odolnosti vůči útokům, které využívají slabiny v konfiguraci. Zajištění souladu s bezpečnostními standardy a doporučeními.

c) Interní penetrační test

- Rozsah - přibližný počet interních systémů / IP adres v testované vnitřní síti. Pokud je součástí testování i Active Directory, tak kolik je v AD uživatelů (přibližně).?

Odpověď: Počet serverů k testování cca 100-150, počet pracovnách stanic k testování cca 500, počet uživatelských účtů v Active Directory cca 500.

- Simulace interního útočníka znamená, že test bude proveden ze stanice Objednatele nebo bude Dodavatel moci využít a zapojit do sítě i svůj HW?

Odpověď: Ze stanice objednatele

- Odposlech komunikace je myšlen na úrovni nakaženého počítače v LAN?

Odpověď: ANO

Odchycení, přesměrování a zneužitím požadujete provedení ARP Poisoning útoku v produkci?
Odpověď: Dle domluvy s vybraným dodavatelem při koordinační schůzce při podpisu smlouvy.

- Je pro interní testy možné využít VPN nebo je vyžadován pouze fyzický přístup?

Odpověď: Je možno využít jak fyzický přístup, tak i VPN.

- Popište cíle testu "spolehlivost konfigurace" pro interní testy.

Odpověď: V kontextu interních penetračních testů se „spolehlivost konfigurace" vztahuje k tomu, jak správně a bezpečně jsou nastaveny systémy, služby a síťové prvky uvnitř organizace. Cílem je odhalit chyby v konfiguraci, které by mohly být zneužity útočníkem s přístupem do interní sítě.

- Popište "pokročilá detekce na odhalení známých či neznámých hrozeb vyskytujících se již v síti objednatele (pokročilý malware, ransomware, apod.)."

- Jedná se o test detekce schopnosti útoku typu ransomware, malware skrze aktivity Dodavatele s tím, že Objednatel ověří kvality svých detekcí?

Odpověď: ANO

- Jedná se analýzu logů a threat hunting aktivit s cílem ověřit, že v síti Objednatele se nevyskytuje pokročilý malware, ransomware? Pokud ano, získá dodavatel přístup k SIEM, EDR apod?

Odpověď: ANO

d) Wi-Fi

- Rozsah - seznam všech testovaných SSID s popisem jejich zabezpečení a účelu použití (např. Návštěvnická WiFi síť, BYOD WiFi síť, Zaměstnanecká WiFi síť).

Odpověď: 3 WiFi sítě (interní, externí a návštěvnická) určené k testu, které jsou zabezpečeny WPA Enterprise

e) Phishing Bude se testovat na zákazníkem dodaném seznamu e-mailů, nebo budeme cílit na veřejně dohledatelné adresy?

Odpověď: Budou předány seznamy e-mailů

- Jedna phishing šablona – plošný test?

Odpověď: ANO – plošný test

- Co se má měřit? Proklik, zadání údajů do falešného formuláře, nebo i odeslání citlivých údajů?

Odpověď: Bude se měřit proklik, zadání údajů do formuláře i odeslání údajů

- Bude použita doména objednatele (vyžaduje SPF/DKIM povolení) nebo doména Dodavatele?

Odpověď: Doména dodavatele

- Budete whiteslitovat domény Dodavatele?

f) USB

- Rozsah - kolik USB disků a kolik lokalit je předmětem testu?

Odpověď: Toto je ponecháno na dodavateli testu – Krajský úřad má v areálu 4 budovy (A, B, C a D; budova A a B s recepcí, budova C – přístup přes vstupní tablo po spojení s daným úředníkem nebo na identifikační kartu, budova D – vstup na identifikační kartu a další 2 místa – patro na budově Zdravotnické záchranné služby – přístup na chip a kanceláře v budově Krajského ředitelství HZS – přístup na klíč a odkódování prostoru pomocí PINu), min. počet USB disků 20.

g) Fyzický test

- Rozsah - Je předmětem testu jedna budova anebo vícero budov, konkrétní prostor (např. kancelář starosty, serverovna, konkrétní poschodí) a konkrétní citlivé informace anebo jejich výběr je na dodavateli testu?

Odpověď: Toto je ponecháno na dodavateli testu.

- O jaký typ neautorizované osoby se jedná?

Odpověď: Osoba mimo úřad s různou úrovní profesionality (profesionální útočník, zkušený zloděj, zvědavý kolemjdoucí)

Dotaz č. 6

Externí infrastruktura

1. Prosím o orientační seznam a stručný popis služeb, které jsou publikovány na IP adresách, které budou předmětem penetračního testování.

Odpověď: inetnum: 194.228.231.0 - 194.228.231.63
inetnum: 85.71.246.0 - 85.71.246.255

2. Preferujete automatizovaný sken zranitelnosti, nebo penetrační test včetně manuální verifikace (exploitace)?

Odpověď: Toto je ponecháno na dodavateli testu.

Dotaz č. 7

Interní infrastruktura

1.Prosím o orientační seznam a stručný popis služeb, které jsou publikovány na IP adresách, které budou předmětem penetračního testování.
Odpověď: Toto bude řešeno s vybraným dodavatelem při koordinování testů
2. Je interní infrastruktura (vnitřní síť) nějakým způsobem segmentovaná?
Odpověď: ANO
3.Pokud ano, bude předmětem testování také prověření segmentace?
Odpověď: ANO
4.Preferujete automatizovaný sken zranitelnosti, nebo penetrační test včetně manuální verifikace (exploitace)?
Odpověď: Toto je ponecháno na dodavateli testu.
5. Uveďte prosím preferovaný přístup k penetračnímu testování interní sítě.
Odpověď: Autentifikovaný uživatel
Toto je uvedeno ve výzvě ve vymezení předmětu plnění veřejné zakázky, tj. simulace útoků útočníkem se známostí, tj. autentifikovaný uživatel.

Dotaz č. 8

Bezpečnostní audit

1. Prosíme o informace, zda má být předmětem nabídky také pravidelný audit kybernetické bezpečnosti dle ZoKB.

Odpověď: Toto je uvedeno ve výzvě ve vymezení předmětu plnění veřejné zakázky, tj. ANO

V souvislosti s tímto vysvětlením č. 3 zadávací dokumentace zadavatel uveřejňuje upravenou přílohu P2 – Návrh smlouvy.

Tímto vysvětlením zadavatel nijak nemění zadávací dokumentaci. Výše uvedené informace pouze upřesňují specifikaci požadovaného plnění. Úpravy zadávací dokumentace nerozšiřují okruh možných dodavatelů, přesto zadavatel prodlužuje lhůtu pro podání nabídek do pátku 31. 10. 2025 do 10:00 hodin. Délka tohoto prodloužení vychází i z toho, že zadavatel již v rámci vysvětlení zadávací dokumentace č. 2 provedl prodloužení doby pro podání nabídek o 7 dnů, a to s ohledem vědomí rozsahu odpovědí v rámci přípravy tohoto vysvětlení zadávací dokumentace.

V Karlových Varech dne 21. 10. 2025