



FRÝDEK~MÍSTEK

Statutární město Frýdek-Místek
Magistrát města Frýdku-Místku
Radniční 1148, 738 01 Frýdek-Místek

**Odbor zadávání veřejných zakázek
pracoviště Radniční 1148, Frýdek**

Váš dopis značka:

Ze dne:

Číslo jednací:

Spisová značka:

Vyřizuje: Bc. Ivo Sztwiertnia

Telefon: 558609292

E-mail: sztwiertnia.ivo@frydek-mistek.cz

Datum: 21.05.2025

VYSVĚTLENÍ ZADÁVACÍCH PODMÍNEK

Veřejná zakázka:	Bezpečnostní a penetrační testy
Evidenční číslo:	P25V00000056
Druh veřejné zakázky:	služby
Zadavatel:	Statutární město Frýdek-Místek Radniční 1148, 738 01 Frýdek-Místek IČ: 00296643, DIČ: CZ00296643

Dotaz č. 1:

VI. test sítě

- dodavatel provede testování sítě provozovaných zadavatelem v budovách (magistrátu) zadavatele
- dodavatel provede testování bezdrátových sítí provozovaných zadavatelem a dostupných v budovách (magistrátu) zadavatele a jeho okolí
- cíle testu budou síťová zařízení, firewally, servery s cílem otestovat, zda lze zneužít chyby v interní síti k získání vyšší úrovně přístupu nebo kompromitaci kritických systémů a přístup k aktivům vnitřní sítě
- předmětem testování bude minimálně:
 - skenování a mapování sítě
 - identifikace zranitelností
 - exploitace služeb
 - zachytávání provozu a útoky typu Man in the middle
 - privilege escalation
 - VLAN hopping
 - DHCP starvation, ARP/MAC spoofing, STP manipulation
 - Apod.

Ze zadání

K testům interní infrastruktury:

- Jaký je řádový počet zařízení v rámci interní sítě (servery, síťová zařízení, koncové stanice, tiskárny apod.)?

Odpověď zadavatele: cca 100 virtuálních serverů, cca 100 síťových zařízení (switche, firewally, AP), cca 500 stanic, cca 200 tiskáren

K testům Wi-Fi:

- Počet bezdrátových sítí, které jsou v scope testu? 4
- Typ zabezpečení jednotlivých sítí v scope testu (Open/WEP/WPA2-PSK/WPA2-Enterprise)?

Odpověď zadavatele: Z důvodu bezpečnosti bude tato informace předána následně po podpisu smlouvy a mlčenlivosti.?

Dotaz č. 2:

VIII. test koncových stanic

- dodavatel provede testování vzorku koncových stanic uživatelů (min. 10)
- předmětem testování bude minimálně:
 - zjistit chybné konfigurace vůči best practice Microsoftu
 - bypassing antivirů a EDR/XDR
 - privilege escalation
- cílem je zjistit, jak lze kompromitovat koncová zařízení zaměstnanců, eskalovat oprávnění a zajistit si přístup ke kritickým částem infrastruktury zadavatele

Většinou testujeme 1 koncovou stanicí (NTB s defaultním nastavením pro zaměstnance). Opravdu je třeba testovat min 10? Mají různá nastavení? Pro nacenění bude prosím třeba přesný počet stanic, který má být otestován.

Odpověď zadavatele: Otestovány budou 4 stanice, kdy se liší jejich konfigurace.

Dotaz č. 3:

IX. test bezpečnosti databázových systémů

- dodavatel provede otestování ochrany databázových serverů (operačních systémů) a samotných databází (Oracle, MSSQL...)
- předmětem testování bude minimálně:
 - zjistit chybné konfigurace vůči best practice
 - brute-force útoky na přihlašovací údaje
 - SQL injection a získání přístupu k datům
 - Privilege escalation
- cílem je zjistit, zda jsou databázové servery a databáze správně chráněny proti neoprávněným přístupům

Ke každé databázi bude třeba vědět velikost (počet tabulek atd.) a počet rolí v databázi.

Odpověď zadavatele: Otestováno bude 5 databázových systémů, počet rolí cca 60, velikost tabulek průměrně 4 tis.

Dotaz č. 4:

Dále jsou to spíš připomínky k zadání, kde máme pocit že je nejednoznačné nebo zadané způsobem, který by vyšel strašně draho a stejného výsledku lze dosáhnout levněji. Poprosím o vyjádření, zda pokračovat s naceněním dle původního zadání, či s našimi úpravami.

Ad I. Rozdělení zaměstnanců na 2 skupiny s různým scénářem a rozdělení těchto skupin na další 4 skupiny s různým časem odeslání nepřinese změny výsledků a zásadní zkomplikuje vyhodnocení kampaně a kampaň prodraží. Kampaň je možné takto nacenit, nicméně finančně výhodnější a efektivnější je skupiny nedělit, a odeslat na všechny zaměstnance dva různé scénáře. Zaměstnanec tak bude testován dvakrát při stejných nákladech. Rozdělení skupin na menší s rozdílným datem odeslání se neosvědčilo, naopak první oslovená skupina z testu vyjde výrazně hůře a další lépe, protože právě efekt vzájemného informování se o kampani, který se má rozdělením odbourat, se zvýší. V případě rozdělení do 4 fází je rizikem i např. zablokování domény nebo její označení některým automatickým systémem za phishingovou a tím ohrožení doručení zbývajících (např. tří) fází.

Odpověď zadavatele: Trváme na nastavených podmínkách.

Dotaz č. 5:

Ad II. Příprava jedné kampaně pro 16 osob (a další pro dalších 16 osob) je opět finančně neefektivní, finančně neefektivní je i rezervace osmi časových slotů pro operátora a osm konfigurací serveru, ze kterého dochází k podvodnému volání. Pokud je cílem navolat 32 zaměstnanců z cca 500, pak lze téhož výsledku dosáhnout jednou kampaní na 32 osob (popřípadě dvěma různými kampaněmi na 32/16 osob).

Odpověď zadavatele: Objednavatel ruší požadavek na rozložení do 4 fází i dvě rozdílné kampaně. Bude realizována pouze 1 podvodná kampaň.

Dotaz č. 6:

Ad III. Rozložení do 4 fází je možné, podléhá ale stejným rizikům. Navrhujeme kampaň na fáze nedělit.

Odpověď zadavatele: Trváme na nastavených podmínkách.

Dotaz č. 7:

Ad IV. Navrhujeme rozdělit na dva body – při průniku (s využitím specialisty na sociální inženýrství) do budovy můžeme hledat slabá místa, kde by se dalo zařízení nepozorovaně připojit, nicméně samotné získání přístupu do infrastruktury vyžaduje specialistu na infrastrukturu a může zabrat více času, a není účelné je dělat skrytě, když může být v rámci bodu VI provedeno při legitimní návštěvě specialisty v budově.

Odpověď zadavatele: Cílem tohoto testu není zjišťování slabých míst jak proniknout do budovy, vzhledem k tomu, že je objednavatel součástí veřejné správy, jsou téměř všechny prostory budovy veřejnosti přístupné. Cílem testu je otestovat odolnost metalické sítě proti nežádoucímu průniku. A taky reakci zaměstnanců na přítomnost někoho manipulujícího s výpočetní technikou ve veřejně dostupných prostorách.

Dotaz č. 8:

Ad V. Pro účely nacenění je potřebná informace, zda je v siti zadavatele implementováno řešení (např. DLP) znemožňující připojení paměťového média k PC. Pokud ano, pak je potřeba využít výrazně dražší zařízení, která tuto technologii obejdou. Pokud ne, je možné využít libovolné USB disky. Dále je pro účely nacenění potřebná informace, zda má analýza (V. druhá odrážka) probíhat skrytou formou, nebo v součinnosti se zaměstnancem úřadu, a rovněž zda na místa analýzou vybraná umístí zařízení zaměstnanec úřadu, nebo je vyžadovaná přítomnost zaměstnance dodavatele.

Odpověď zadavatele:

Objednavatel umožní připojení libovolného paměťového média – USB disku. Nicméně před samotným doručením, musí dojít k otestování funkčnosti řešení – zaslání informace zdali byl USB disk vložen do PC (tak aby nedošlo k případné blokaci antivirovým systémem, EDR, firewallem atd.)

Dotaz č.9

V článku 5 odst. 6. Smlouvy o poskytnutí služeb (dále jen „Smlouva“) je uvedeno, že *Ujednáním o smluvních pokutách není dotčeno právo poškozené smluvní strany na náhradu škody v plné výši, přičemž za škodu se považuje i ušlý zisk včetně přiměřeného zadostiučinění pro případ poškození dobrého jména města.*

Dle názoru dodavatele je takový požadavek nepřiměřený. Nelze po dodavateli spravedlivě požadovat, aby nesl odpovědnost za případnou škodu v plné výši. Nelze totiž z podstaty věci dopředu odhadnout, jak vysoká by mohla případná škoda být. Důvodová zpráva k občanskému zákoníku uvádí, že rozsah náhrady škody podmiňuje její předvídatelnost. Dle názoru dodavatele nemůže být výše škody v daném případě předvídatelná a může být zcela nepřiměřená míře rizika, kterou je dodavatel ochoten na sebe převzít při plnění veřejné zakázky. Požadavek na nijak nelimitovanou náhradu škody je tedy nepřiměřený hodnotě veřejné zakázky. Tím dochází k porušení zásady přiměřenosti uvedené v § 6 ZZVZ. Dodavatel nemůže dopředu výši škody předvídat a toto riziko musí promítat do nabídkové ceny.

Dodavatel má za to, že ke stanovení neomezené odpovědnosti za škodu neopravňují zadavatele ani charakter, hodnota a význam zajišťovaných povinností, ani vzájemný poměr hodnoty zajišťovaného závazku a výše škody. Dodavatel apriori nepředpokládá, že bude porušovat své povinnosti ze smlouvy, ovšem přesto má za to, že je neomezená náhrada škody nepřiměřená. Dodavatel apeluje na zadavatele, aby ještě zvážil funkci náhrady škody při posuzování přiměřenosti její výše a přihlédl k celkovým okolnostem úkonu, jeho pohnutkám a účelu, který byl zadavatelem sledován.

Dodavatel si je vědom toho, že jednou ze základních povinností zadavatele je jednat s péčí řádného hospodáře, a tím i zajistit pokrytí eventuálních škod, jež by mu mohly vzniknout z porušení smluvního vztahu, nicméně z toho automaticky nevyplývá povinnost požadovat neomezenou náhradu škody po dodavateli ve veřejné zakázce. Dodavatel upozorňuje zadavatele, že jedinou možností dodavatele jakožto řádného hospodáře je navýšit tzv. „risk budget“ na co nejvyšší možnou částku (jelikož nezná výši případné škody). Náklady na tento risk budget pak budou rozprostřeny do nabídkové ceny.

Zadavatel si musí být vědom toho, jaká maximální škoda by mohla teoreticky vzniknout, kdy jako řádný hospodář by mohl škodu limitovat výší s dostatečně velkou rezervou, aniž by musel být neomezená. Takto bude zadavatel z veřejných prostředků sanovat náklady na risk budget. Pokud bude zadavatel tyto náklady přenášet na dodavatele, pak měl zadavatel tyto náklady zakalkulovat do předpokládané hodnoty veřejné zakázky, a navýšit ji.

Upraví tedy zadavatel Smlouvu tak, že doplní limitaci výše škody, kterou bude oprávněn na dodavateli požadovat, a to maximálně do výše ceny za předmět plnění?

Odpověď zadavatele:

Zadavatel nebude limitovat škody, které mohou zadavateli vzniknout činností dodavatele (např. při zneužití/úniku dat a následném kybernetickém útoku). Ustanovení smlouvy o náhradě škody vyplývá z ustanovení zákona č. 89/2012 Sb., občanský zákoník, v platném znění. Pokud by příslušné ustanovení o náhradě škody v plné výši ve smlouvě uvedeno nebylo, postupovalo by se v případě sporu podle příslušných ustanovení občanského zákoníku, která jsou obdobná ustanovením předmětné smlouvy, a to dle ust. § 2913 občanského zákoníku, které právě řeší základní předpoklady pro odpovědnost za škodu při porušení smluvní povinnosti - „*Porušili strana povinnost ze smlouvy, nahradí škodu z toho vzniklou druhé straně nebo i osobě, jejímuž zájmu mělo splnění ujednané povinnosti zjevně sloužit.*“

Pokud dodavatel ve svém dotazu poukazuje na text důvodové zprávy ve vztahu k „předvídatelnosti“ škody, pak k tomuto lze uvést, že důvodová zpráva k občanskému zákoníku na str. 569 skutečně uvádí, že „*Rozdíl mezi smluvní a mimosmluvní povinností k náhradě škody jsou zejména v tom, že se pro vznik povinnosti nahradit škodu porušením smlouvy nevyžaduje zavinění a že rozsah náhrady škody podmiňuje její předvídatelnost,*“ avšak hned navazující věta důvodové zprávy pokračuje tak, že „*Ustanovení § 2913 občanského zákoníku o předvídatelném rozsahu škody mlčí vzhledem k výsledku diskusí v komisích Ministerstva spravedlnosti i v ústavněprávním výboru Poslanecké sněmovny, kde převládlo stanovisko, že v daném případě postačuje teorie adekvátní příčinné souvislosti.*“

Dodavatel je plně odpovědný za služby, které coby profesionál poskytuje za úplatu. Sdělení, že dodavatel není ochoten nést plnou odpovědnost za své služby, je u tak významného dodavatele zarážející. Nadto zadavatel předpokládá, byť to nestanovil jako podmínku účasti v tomto výběrovém řízení ani jako smluvní podmínku, že dodavatel jako podnikající subjekt v tomto dnes dynamickém a současně rizikovém oboru má jistě sjednáno odpovídající pojištění odpovědnosti za škodu s limitem pojistného plnění, které koreluje s jeho předmětem činnosti, resp. objemem jeho smluvních závazků, které na sebe převzal.

Pokud dodavatel uvádí, že *nemůže být výše škody v daném případě předvídatelná a může být zcela nepřiměřená míře rizika, kterou je dodavatel ochoten na sebe převzít při plnění veřejné zakázky. Požadavek na nijak nelimitovanou náhradu škody je tedy nepřiměřený hodnotě veřejné zakázky. Tím dochází k porušení zásady přiměřenosti uvedené v § 6 ZZVZ. Dodavatel nemůže dopředu výši škody předvídat a toto riziko musí promítat do nabídkové ceny.* ", pak s těmito názory či spíš polemikou zadavatel nesouhlasí.

Dodavatel zaměňuje smlouvu, resp. její předmět plnění, včetně její hospodářské kauzy závazku a tedy i samotné zakázky, na kterou dopadá její předpokládaná hodnota s institutem náhrady škody, který je pojmově sekundární - odpovědnostní, byť jeho základ tkví a je odvozený ze smlouvy, resp. následků porušení smlouvy, popřípadě ex delicto v případě mimosmluvní odpovědnosti za škodu. Již z tohoto důvodu je argumentum ad absurdum nemyslitelné, aby zadavatel do předpokládané hodnoty zahrnoval tyto případné sekundární nároky, které ani nepoptává a ani nemůže poptávat - stěží si lze představit, že předmět požadavku zadavatele na plnění veřejné zakázky by zněl, aby vedle splnění závazku „způsobil dodavatel zadavateli škodu !“ Při takové konstrukci - samozřejmě dovozené ad absurdum - by předpokládaná hodnota převážné části veřejných zakázek způsobila, že by spadaly do podlimitního či spíše nadlimitního režimu, přitom i při jakékoli veřejné zakázce nepatrné hodnoty, může být dodavatelem na majetku zadavatele způsobena škoda vysoko převyšující předpokládanou hodnotu.

O to víc se dodavatel mylí, když institut náhrady škody považuje za zajišťovací institut, když uvádí, že „*Dodavatel má za to, že ke stanovení neomezené odpovědnosti za škodu neopravňují zadavatele ani charakter, hodnota a význam zajišťovaných povinností, ani vzájemný poměr hodnoty zajišťovaného závazku a výše škody*“....., ačkoliv jde o základní princip občanskoprávních vztahů tradičně označovan v právní teorii a nauce zkráceně – **neminem laedere** – nikomu neškodit/nikoho nepoškozovat, a když toto porušení nastane, pak povinnost škůdce odškodnit, tedy je zásadně institut reparační, restituční u škody na věci, resp. v případě imateriální újmy plní i funkci satisfakční.

Pro úplnost zadavatel dodává, že nikterak tímto netvrdí, že při rozsahu náhrady škody nehraje roli předvídatelnost její výše způsobené v občanskoprávních vztazích zde podle § 2913 OZ, byť není jako pojmový zákonný znak explicitně v tomto ustanovení vyjádřen, nicméně bude v aplikační praxi dovozován v rámci teorie adekvátní příčinné souvislosti, což plyne nejen z citované důvodové zprávy ale i z řad odborných publikací a článků k této problematice.

V kontextu výše podaného vysvětlení zadavatel nespatřuje žádný prostor, ani důvod, jakkoliv limitovat výši škody, jak navrhuje tazatel.

Příloha Specifikace předmětu plnění byla aktualizována.

V důsledku změny zadávacích podmínek se lhůta pro podání nabídek prodlužuje do 2. 6. 2025, do 9:00 hodin.

Mgr. Roman Šebesta

vedoucí odboru zadávání veřejných zakázek