Zadavatel **:** Město Nové Město na Moravě
Vratislavovo nám. 103, 592 31 Nové Město na Moravě
IČ: 00294900

Vysvětlení zadávací dokumentace č.1

název veřejné zakázky:

„Penetrační testy v rámci projektu „Zvýšení odolnosti DC proti kybernetickým hrozbám“

Zadavatel na základě žádosti zveřejňuje vysvětlení zadávací dokumentace k výše uvedené veřejné zakázce:

Dotazy:

1. Termín odevzdání je 16.3.2024, 11.00 hod. Jde o termín v minulosti, prosíme o opravu.

2. Je možné umístit do lokality objednatele zařízení (PC), ke kterému se následně budeme vzdáleně připojovat? Nebo je očekávána fyzická přítomnost v prostorách objednatele po celou dobu testu? Pokud ano, kde jsou tyto prostory umístěny?

3. Pro provedení testů používáme nástroje třetích stran, mj. skenery zranitelností a i autonomní penetrační nástroj, který využívá AI. Před spuštěním tohoto testu je nutné odsouhlasit všeobecné obchodní podmínky vendora, jejichž součástí je i NDA. Je to proto, že externí testování se provádí z prostředků vendora a tudíž je nutné vyjasnit právní rámec tohoto jednání. Je toto za objednatele akceptovatelné?

4. Ve smlouvě nám chybí prohlášení objednatele, že je výhradním vlastníkem všech předaných IP adres a předmětů testování a požadovanými testy nebude zasaženo do práv třetích osob. Pokud by bylo toto prohlášení nepravdivé, pak bude objednatel povinen nahradit všechny nároky uplatněné třetími osobami za poskytovatele.

- z pozice dodavatele nedokážeme posoudit, nakolik jsou předaná aktiva správná. Penetrační testování je citlivá aktivita, při níž je možné způsobit škodu i vytvořit možnou trestněprávní zodpovědnost. Je možné nějaké podobné prohlášení doplnit, nebo si je objednatel vědom těchto skutečností a považuje je za automatické?

5. Jak je definovaná pracovní doba objednatele?

6. Prosíme o poskytnutí informace zmíněné v bodu 11.15.: Tato smlouva byla uzavřena v souladu s usnesením Rady města Nové Město na Moravě přijatým na její schůzi č. 10 konané dne 15.5.2023 pod bodem č. 31/10/RM/2023.

7. Prosíme o vysvětlení vztahu externích penetračních testů a bodu 8.1 - poskytnutí přístupu do WiFi sítí. V definici externího penetračního testu není zmíněno testování WiFi sítí a není uvedeno ani v kapitole Rozsah penetračního testování. Dle běžných standardů jde o zvláštní kategorii testů. Pokud objednatel předpokládá i

testování WiFi sítí, prosíme o náležitou úpravu smlouvy, poskytnutí mapy pokrytí, sdělení počtu WiFi Access Pointů a počtu ESSID, které mají být předmětem testování.

8. V technické specifikaci je v rámci aktivit uvedeno odstranění nálezů. Je uveden i retest. Ve smlouvě je ale pevný termín 15.5.2024 a ve smlouvě není problematika retestů nijak upravena. Pokud je reakční doba objednatele až 5 dní, není, pokud se má penetrační test provést řádně, možné v termínu zakázku realizovat. Prosíme o vysvětlení, jak objednatel provedení retestů zamýšlel a také o vysvětlení očekávaných pravidel retestu ve smlouvě.

9. Proběhl už v minulosti nějaký penetrační test? Pokud ano, byly všechny nálezy odstraněny?

- (Nálezů může být velké množství a retest tak může být velice časově náročný, což výrazně ovlivní cenu výsledného díla. Doporučujeme požadavek na retest omezit nějakým počtem MD, aby nabídky mohly být porovnatelné.)

10. Prosím o popis toho, co objednatel rozumí pod aktivitami závěrečná zpráva a vyhodnocení testu. Běžně vyhodnocení testu sepisujeme do závěrečné zprávy a následně prezentujeme, nerozumíme proto těmto požadovaným bodům, které nejsou definované v zadávací dokumentaci. Prosíme o jejich vysvětlení.

11. Prosíme o kontrolu odkazu z technické dokumentace: Detailní metodika dle: 2022-03-07_Penetracni-testovani_v1.2.pdf Materiál je nazván Úvod do problematiky popisující penetrační testy a jejich možnosti a obecně popisuje problematiku penetračních testů. Je tento uvedený materiál správný?

12. Prosíme o zaslání počtu (nikoliv seznamu) IP adres, které mají být předmětem interního a externího penetračního testování .

Odpověď:

1) ano, překlep, upřesněno ve zveřejněných dodatečných informacích na profilu zadavatele dne 8.4.2024

2) Ano je-li to nutné je možno umístit zařízení a je k němu prostřednictvím VPN přistupovat, nebo přistupovat skrze VPN do infrastruktury objednatele vzdáleně. Adresa: Městský úřad, Vratislavovo náměstí 103, 592 31 Nové Město na Moravě, 2 NP.

3) Uzavření NDA smlouvy není problém, nicméně smlouvu nemáme k dispozici a při uzavírání smlouvy může dojít k standardnímu schvalovacímu procesu, který je závislý na termínech jednání rady města.

4) Objednatel si je plně vědom těchto skutečností. U IP rozsahů, u kterých není město zcela výhradním vlastníkem je s ISP běžně v kontaktu a informuje je předem o zahájení testů, která si objednává, nebo je účastníkem pravidelného testování z národního CSIRT.

5)
Úřední hodiny:
Pondělí 08.00 – 18.00
Středa 08.00 – 17.00
Čtvrtek 08.00 – 14.00
Provozní doba:
Úterý 07.30 – 15.00
Pátek 07.30 – 13.00

6) 31/10/RM/2023 Pověření starosty/místostarostů k podepisování smluv

7) Jedná se o překlep- zapomenutý text, žádné WiFi sítě nejsou součástí tohoto penetračního testování.

8) Retestování je popsáno jako následující logický krok po provedení penetračních testů. A zaměřuje se na chyby a problémy z poptávaného penetračního testu, který určí jejich závažnost a tím i nutný termín k jejich odstranění. Provedení retestování bude řešeno navazující objednávkou dle výsledků penetračního testu. Vzhledem k detailnímu nevyhovujícího stavu vzešlého z penetračního testu se lze cíleně zaměřit na konkrétní hrozby a provádět tak již testování odhalených zranitelností. V aktivitách je odstranění nálezů správně uvedeno, jelikož se jedná vždy o úzkou součinnost mezi dodavatelem a objednatelem při nápravě nevyhovujícího stavu.

9) Ne jelikož se jedná o zcela novou dodávku HW a SW, která nemohla být v minulosti testována. Vzhledem k tomu, že zadavatel není schopen posoudit jaké jsou technologické možnosti použité pro penetrační testování a jakou techologii dodavatel zvolí, nebyly určeny žádné konkrétní užší rámce.

10) Objednatel vychází z podpůrných materiálů Penetračního testování NUKIB, kde jsou tyto body definovány takto:

5.5 Závěrečná zpráva
Jedná se o dokument, který je poskytnut objednateli jako důkaz o tom, co bylo vykonáno. Existují případy, kdy je snaha odevzdat sken zranitelností jako výstup penetrační testování. Jedná se však o odlišné procedury, které nelze vzájemně zaměňovat. Výstup ze skenování zranitelností není závěrečnou zprávou penetračního testování.

Závěrečná zpráva zpravidla obsahuje:
• *manažerské shrnutí,*
• *harmonogram testu,*
• *přesné zadání testu,*
• *omezení testu,*
• *použitou metodologii,*
• *nalezené problémy,*
• *detailní popis zranitelností,*
• *doporučení k odstranění nálezů,*
• *přehledové tabulky (tabulka nálezů, tabulka systémů apod.).*

5.6 Vyhodnocení testu
Po provedení penetračního testování je potřeba prodiskutovat nálezy.
Dále je potřeba jednotlivé nálezy posoudit v kontextu samotné organizace, určit priority k nápravě a zadat jednotlivé úkoly.

https://nukib.gov.cz/download/publikace/podpurne_materialy/2022-03-07_Penetracni-testovani_v1.2.pdf

11) Ano je, zadavatel se snažil v zadávací dokumentaci odkázat na dokument, který je vytvořen nekomerčním subjektem, a kterým by se měl případný dodavatel rámcově řídit. Slovo metodika je v zadání použita nadbytečně.

12) Externě 126 - Interně 280

8.4.2024

Mgr. Daniela Krejčí
admin.VZ

Mgr. Daniela Krejčí
Digitálně podepsal Mgr. Daniela Krejčí
Datum: 2024.04.08 16:15:14 +02'00'