Technická specifikace

je jednou z příloh ke zveřejněné veřejné zakázce s názvem
„**Penetrační testy (2025)**“

Uchazeč je povinen vyplnit ve všech tabulkách vždy sloupec s označením *„Nabízené plnění*“, a to tak, že vyplní příslušný parametr nebo údaj, který je součástí nabídky, který však nesmí mít nižší hodnotu, než požaduje zadavatel ve sloupci „*Požadavek zadavatele*“. Pokud by parametr měl nižší hodnotu, je to důvodem k vyřazení nabídky uchazeče. U číselně vyjádřitelných hodnot je uchazeč povinen nabídnout pouze jednu hodnotu.

1. Identifikační údaje	
1.1. Zadavatel	
Název:	Město Vsetín
Sídlo:	Svárov 1080, 755 24 Vsetín
IČ:	00304450
DIČ:	CZ00304450
Osoba oprávněná jednat jménem zadavatele:	Jiří Čunek, starosta města
Kontaktní osoba:	[redacted]
Tel./fax:	
E-mail:	
1.2. Dodavatel	
Název:	*Trusted Network Solutions, a.s.*
Sídlo/místo podnikání:	*Ptašínského 309/6, 602 00, Brno Česká republika*
Osoba oprávněná jednat za uchazeče:	[redacted]
Kontaktní osoba:	
Tel./fax:	
E-mail:	

2. Technická specifikace	
Položka – požadavek zadavatele	***Nabízené plnění (výrobce, SW produkt, číselné nebo slovní vyjádření, hodnota, shoda s požadavky – ANO / NE)***
2.1 Penetrační testy (PT) – pro ověření aplikační bezpečnosti informačních systémů zadavatele.	
Penetrační testování je závěrečnou etapou projektu *„Zvýšení kybernetické bezpečnosti města Vsetín“*, cílem penetračního testování je ověřit naplnění technických opatření dle vyhlášky 82/2018 Sb., o kybernetické bezpečnosti, konkrétně opatření uvedených v *§ 18, 22, 23, 25 a §27*. Penetrační testování tak bude sloužit jako nezávislé ověření, že nově implementovaná opatření (*NGFW, Fortinet switche, dohledový systém Elisa, záložní serverovna, backup server a pásková jednotka*) naplňují výše jmenované paragrafy této vyhlášky a plní účel poskytnuté dotace ze strany dotačního orgánu. Výstupem penetračního testování nebude pouze identifikace zranitelností, ale také prokazatelné ověření, že technická opatření přijatá v souvislosti s realizovanými veřejnými zakázkami naplňují výše	*Nabízené penetrační testování bude provedeno v režimu vzorkového ověření souladu dle § 18, 22–24, 25 a 27 vyhlášky č. 82/2018 Sb., tj. formou praktického ověření funkčnosti implementovaných opatření, bez realizace plošného skenování celé infrastruktury, bez fyzických testů a bez aktivních DoS či sociálně-inženýrských útoků.* *§ 18 – Bezpečnost komunikačních sítí* *Nabízené plnění:* *Prověření segmentace sítě a řízení přístupu mezi VLAN pomocí Fortinet NGFW a switchů Fortinet.* *Součástí je vzorkové ověření komunikace mezi uživatelskou, serverovou a admin VLAN, ověření blokace vybraných portů a VPN konfigurace.* *Test bude proveden kombinací automatizovaného a manuálního ověření dle standardu PTES.* *Shoda s požadavky: ANO.*

jmenovanou vyhlášku – např. NG firewall blokuje škodlivé porty, síť je segmentována podle definovaných pravidel.
 	
Výstup ve formě závěrečné zprávy bude sloužit jako doklad o provedení technických opatření, která zvyšují zabezpečení informačních a komunikačních systémů města Vsetín.
 	
Základní požadavky na penetrační testování podle vyhlášky 82/2018 Sb.:
 	
§ 18 – Bezpečnost komunikačních sítí
• ***Požadavek vyhlášky:*** Segmentace sítě, řízení přístupu, centrální správa.
• ***Stav před realizací projektu:*** Městská síť byla historicky plochá, bez segmentace.
• ***Realizovaná opatření:*** Nově nasazený nextgen Firewall Fortinet a switche Fortinet, umožní vytvořit segmentaci sítě a řízení přístupu mezi jednotlivými VLANy.
• ***Cíl penetračního testu:*** Ověřit, že nové síťové prvky skutečně provádí segmentaci a chrání jednotlivé VLANy.
• ***Penetrační test bude zahrnovat:***
  • Pokus o průnik z uživatelské VLAN do serverové nebo admin VLAN.
  • Kontrola blokace škodlivých portů a služeb na NGFW.
  • Ověření správného nastavení VPN.
• **Očekávaný výstup:** NGFW blokuje nepovolené porty, VLAN segmentace funkční, neautorizovaný přístup mezi segmenty není možný.
 	
§ 22–24 – Logování a detekce událostí
• ***Požadavek vyhlášky:*** Sběr a vyhodnocování logů.
• ***Současný stav:*** Decentralizované logování, nově nasazen dohledový systém Elisa (naplňující SIEM a provozní monitoring, dále součástí projektu je Fortinet Analyzer pro logování, analýzu a reporting).
• ***Cíl penetračního testu:*** Ověřit, že Elisa a Fortinet Analyzer detekuje podezřelé události a administrátor je notifikován. Dále ochranu logů před jejich smazáním.
• **Očekávaný výstup:** Dohledový systém zaznamenal a vyhodnotil testovací incident, administrátor obdržel notifikaci e-mailem.
 	
§ 25 – Aplikační bezpečnost
• ***Požadavek vyhlášky:*** Zajistit bezpečnost aplikací, zejména těch, které jsou dostupné z internetu. V případě dostupnosti provádět penetrační testy aplikací.
• ***Současný stav:*** V počítačové síti zadavatele jsou agendové informační systémy dodávané různými dodavateli. Některé jako např. GIS, poskytuje své služby i do internetu.
• ***Cíl penetračního testu:***
• Ověření nastavení šifrované komunikace (SSL/TLS šifrování).
• Náchylnost k DoS/DDoS útokům.
	§ 22–24 – Logování a detekce událostí
	
	Nabízené plnění:
	Modelová simulace bezpečnostního incidentu pro ověření zachycení a notifikace události v systémech Elisa a Fortinet Analyzer.
	Součástí je ověření funkčnosti sběru logů a základního vyhodnocení událostí, včetně ochrany proti mazání záznamů.
	Shoda s požadavky: ANO.
	
	§ 25 – Aplikační bezpečnost
	
	Nabízené plnění:
	Penetrační test agendové webové aplikace dostupné z internetu (např. GIS) formou grey-box testu.
	Rozsah dle OWASP Top 10 – ověření šifrování (SSL/TLS), autentizace, session managementu a základní odolnosti vůči DoS útokům (bez aktivního provádění).
	Shoda s požadavky: ANO.
	
	§ 27 – Zajištění dostupnosti informací
	
	Nabízené plnění:
	Ověření funkčnosti bude provedeno formou kontroly konfigurace zálohovací politiky a protokolů obnovy, nikoli fyzickým provedením restore.
	Shoda s požadavky: ANO.
	
	Doplňující požadavky
	
	Testování bude realizováno dle mezinárodně uznávaných metodik PTES, OSSTMM a OWASP. Výstupem bude manažerská a technická zpráva včetně klasifikace nálezů podle CVSS, doložení postupu testování a doporučení nápravných opatření.

- Možnost zneužití aplikace neautorizovaným způsobem (např. SQL Injection).
- Získání citlivých informací z testovaných informačních systémů zadavatele.
- Zneužití zranitelností pro získání přihlašovacích údajů uživatelů do informačních systémů zadavatele.
- Posoudit, zda zranitelnosti známé z *OWASP Top 10* nejsou přítomny.

- **Očekávaný výstup:** Testované aplikace neobsahují kritické zranitelnosti (např. SQL Injection). Veškerá komunikace probíhá přes šifrované protokoly, session je správně řízená a nelze jí zneužít.

§ 27 – Zajištění dostupnosti informací

- ***Požadavek vyhlášky:*** Dostupnost, odolnost, zálohování, obnova.
- ***Současný stav:*** Nasazen nový backup server, pásková jednotka a záložní serverovna. Omezení nedostupnosti služeb při výpadku hlavní serverovny.
- ***Cíl penetračního testu:***
- Ověřit, že zvolená zálohovací strategie (zálohování přes aplikaci Veeam a uložení na magnetické pásky) je funkční a že záloha lze obnovit na záložní server.

- **Očekávaný výstup:** Úspěšná obnova dat z poslední zálohy pro failover cluster do záložní serverovny je funkční.

Doplňující požadavky na penetrační testování:

– **Režimy penetračního testování:**

- ***Black-box:***
  Penetrační tester nemá k dispozici žádné informace o infrastruktuře a použitých technologií.

- ***Grey-box:***
  Zahrnuje předání základních informací o architektuře sítě a použitých technologií.

– **Přístup k testovanému prostředí zadavatele:**
- ***Fyzicky (onsite)*** na infrastruktuře se svým zařízením.
- ***Vzdáleně (remote)*** *pomocí* přístupu na testovací zařízení.
- Přístup bude realizován v souladu s vnitřními bezpečnostními směrnicemi a legislativou, a v režimu, který neohrozí běžný chod organizace.

– **Účel penetračního testování:**
- Ověřit, zda lze proniknout do informačních systémů provozovaných organizací prostřednictvím testování zranitelností, chybného nastavení softwaru nebo hardwaru.
- Ověřit, zda jsou v softwarových a hardwarových prvcích informačního systémů přítomny známe zranitelnosti.
- Ověřit, zda lze proniknout do informačního systému pomocí metod sociálního inženýrství.

- Identifikovat a analyzovat zranitelnosti v infrastruktuře zadavatele a odhalit slabá místa, která by mohla ohrozit důvěrnost, integritu nebo dostupnost dat.
- Zpracovaní návrhu na odstranění identifikovaných zranitelností.

– **Požadavky na průběh testování:**
- Testy musí být provedeny způsobem, který neohrozí běžný denní provoz organizace.
- Testy mohou být provedeny i mimo běžnou pracovní dobu organizace včetně víkendů.
- V případě vážného problému (nálezu) musí být zadavatel informován i před sestavením finálního manažerského i technického výstupu penetračního testování.
- Testování zahrnuje všechna dostupná IP zařízení tvořící infrastrukturu zadavatele.

– **Metodika a postup testování:**
Penetrační testy budou prováděny v souladu s mezinárodně uznávanými standardy s cílem ověřit aplikační bezpečnost informačních systémů zadavatele a identifikovat zranitelnosti infrastruktury, konfigurací a aplikací.

- **PTES** – (Penetration Testing Execution Standard)
- **OSSTMM** – (Open-Source Security Testing Methodology Manual).
- **OWASP** – (The Open Web Application Security Project).

– **Minimální rozsah penetračních testů:**

- ***Identifikace cíle, prostředí a hledání zranitelností*:** sběr informací o cíli, identifikace používaných a aktivních IP adres, detekce síťových služeb, operačních systémů a aplikací, výběr možných perspektivních cílů atd.).
- ***Provedení automatických i ruční skenů (testů):*** po získání dostatečného množství informací probíhá testování jako semi-automatické, kdy jsou využívány nástroje detekce zranitelností a jejich manuální vyhodnocení. Zároveň jsou provedeny i ruční testy pro odhalení komplexnějších zranitelností.

– **Součinnost smluvních stran během penetračních testů**
- Zadavatel zajistí přístup k testovaným zařízením a datům.
- Vzájemná součinnost při stanovení termínů a harmonogramu testování.
  Definování kontaktních osob a eskalačního kontaktu pro případ kritického nálezu.

– **Výstupy a ochrana dat:**
- Zpráva popisující výsledky testování a návrh opatření k prevenci opakování útoků.
- Veškerá data z testování zůstávají v prostředí zadavatele.
- Předání výsledků bude zabezpečeno šifrováním, přístup bude pouze autorizovaným osobám

– **Použité nástroje pro penetrační skenování:** Předpokládá se, že penetrační tester je držitelem licencí k softwaru nespadající do kategorie open source. Technická analýza bude zahrnovat informace o použitých nástrojích. • ***Open source*** (Nmap, WireShark, SQLmap atd.). • ***Komerční software*** (např. Burp Suite Pro). – **Závěrečná zpráva penetračních testů:** Závěrečná zpráva je hlavním výstupem provedeného penetračního testování. Závěrečná zpráva by měla pokrýt manažerskou i technickou část: • **Manažerské shrnutí** – přináší strategické informace a přehled o slabých místech, která mohou být využita k průniku do testovaných systémů. Zároveň definuje stupeň jejich závažnosti a navrhuje doporučená nápravná opatření. • **Technická analýza** – obsahuje detailní technický popis zjištěných nálezů, včetně podrobných informací o zranitelnostech, důkazů o jejich zneužitelnosti a případného checklistu k nápravě nalezených problémů. • **Popis metodiky a technik** – obsahuje časovou osu průběhů testů, příklady úspěšných útoků. Nalezené bezpečnostní nedostatky a zranitelnosti jsou klasifikovány pomocí pětibodové stupnice dle metodiky **CVSS** (informativní / nízká / střední / vysoká / kritická), která vyjadřuje úroveň rizika. V případě zjištění **kritické zranitelnosti** v průběhu testování jsou tyto informace bezodkladně předány odpovědným osobám na straně zadavatele. ***Seznámení a diskuze nad nálezy PT může být osobně nebo online přes aplikaci jako je např. MS Teams.***	

3. Osoba oprávněná jednat za uchazeče	
Titul, jméno, příjmení	Mgr. Peter Šinaľ
Funkce	člen představenstva & CEO
Podpis oprávněné osoby, razítko