**Název zakázky:** Bezpečnostní a penetrační testy
**Číslo zakázky:** P25V00000056
**Zadavatel:** Statutární město Frýdek-Místek, se sídlem Frýdek-Místek, Radniční 1148, PSČ 738 01

## 1. Cena dodávky

| | Cena celkem bez DPH | DPH | Cena celkem včetně DPH |
|---|---|---|---|
| Penetrační a bezpečnostní testy | 339 000 | 71 190 | 410 190 |
| **CELKEM** | 339 000 | 71 190 | 410 190 |

## 2. Technická specifikace předmětu plnění veřejné zakázky

Předmětem zakázky je dodání služby, pomocí které budou provedeny bezpečnostní a penetrační testy interní infrastruktury a sociální inženýring s cílem identifikovat slabá místa, prověřit zabezpečení aplikací a infrastrukturních prvků a dále ověřit, zda:

- lze získat neoprávněný přístup k službám, datům či informačním systémům objednatele,
- lze neoprávněně modifikovat nebo zničit data objednatele,
- lze narušit dostupnost služeb nebo informačních systémů objednatele,
- lze získat autentizační údaje zaměstnanců objednatele či jiných osob,
- lze zneužít ICT infrastrukturu objednatele,

a poskytnout o tom důkazy. Veškeré testy musí být prováděny nedestruktivně tak, aby nedošlo ke ztrátě nebo porušení dat nebo dlouhodobému výpadku služby. Výsledky testů musí být kvantifikovatelné, opakovatelné a založené na faktech zjištěných během testování. Reportované výsledky musí obsahovat informace o potenciálním riziku, konkrétním postupu nápravy a pravděpodobnosti zneužití v praxi.

Otestována by měla být veškerá zařízení dostupná po síti v době testů vyjma koncových stanic uživatelů, u kterých stačí vhodně zvolený reprezentativní vzorek. Testy budou předem konzultovány s objednatelem, který poskytne potřebnou součinnost. Testování se bude provádět pouze ve stanovených dnech a časech, a z IP adres schválených objednatelem.

Dodavatel je povinen zajistit bezpečnost dat a výstupů vzniklých během testování. Fyzické kopie výsledků musí být chráněny a přístupné pouze autorizovaným osobám. Při předávání výsledků musí být použity kryptografické metody šifrování.

Po skončení testu bude celé prostředí uvedeno do původní stavu, veškeré uložené skripty či modifikace infrastruktury budou navráceny do stavu před započetím penetračního testu. Bezpečnostní a penetrační testy musí být provedeny v níže požadovaném rozsahu a musí splňovat veškeré níže uvedené požadavky na formy, metody, režimy, postupy a vyhodnocení.

### a) Požadavky na režimy testování

Testování bude probíhat v režimu tzv. gray-box testu, kdy dodavatel služby dostane od objednatele k dispozici částečné informace o organizační struktuře, interních a externích procesech, personálně organizačních opatřeních a strukturách, architektuře sítě, konfiguraci informačních systémů a poskytovaných službách, které budou nezbytné k poskytnutí služby.

Testování by mělo simulovat reálné útoky přiměřeně finančně motivovaného externího útočníka, proto všechny testovací scénáře budou v režii dodavatele, objednatel tedy neposkytne součinnost při vymýšlení scénářů a specifik testovacích útoků.
Objednatel předpokládá převážně manuální testování s využitím automatických nástrojů a metod v relevantních částech testů. Výstupy testů nesmí obsahovat pouze výstupy z automatických scanů nástroji typu Nessus, Nmap a další, ale musí obsahovat i manuální ověření nálezů. U testů, u kterých to je relevantní, musí být test realizován ve všech oblastech metodiky OWASP Testing Guide.

### b) Požadavky na metody testování

Objednatel požaduje provedení všech těchto metod a testů:

#### I. e-mailový test – tzv. phishing

- test bude dodavatelem proveden prostřednictvím elektronické pošty
- před ostrým spuštěním musí proběhnout test, zdali budou emailové zprávy doručeny uživatelům skrze bezpečnostní prvky zadavatele
- rozsah testu:
  - minimálně 2 rozdílné podvodné kampaně, kdy každá bude časově rozložena do 4 fází
  - časové fáze budou sloužit rovněž k rozložení útoku mezi uživatele sdílející stejné prostory/kanceláře pro zvýšení důvěryhodnosti útoku
  - celkový počet uživatelů 500 (250 na každou kampaň)
  - uživatelé budou vybráni zadavatelem
- dodavatel musí v obou kampaních využít simulovaného podvodného webu, či webové aplikace navržené přímo pro účely podvodné kampaně, které budou schopny odchytit přihlašovací údaje uživatelů

#### II. telefonický test – tzv. vishing

- test bude dodavatelem proveden prostřednictvím telefonického hovoru
- před ostrým spuštěním kampaní musí proběhnout testovací hovor se zaměstnancem odboru informačních technologií zadavatele, pro ověření a slazení názvosloví, používaných výrazů, informací o provozovaných systémech atd.
- rozsah testu:
  - 1 kampaň
  - celkový počet uživatelů 32
  - uživatelé budou vybráni zadavatelem
  - u uživatelů s více telefonními kontakty budou preferována čísla pevných linek

#### III. sms test – tzv. smishing

- test bude dodavatelem proveden prostřednictvím krátkých textových zpráv (SMS)
- před ostrým spuštěním kampaně musí proběhnout test se zaměstnancem odboru informačních technologií zadavatele, pro ověření a slazení názvosloví, používaných výrazů, informací o provozovaných systémech atd.
- rozsah testu:
  - 1 podvodná kampaň, časově rozložená do 4 fází
  - celkový počet uživatelů 100

- uživatelé budou dodavatelem vybráni ze skupin uživatelů, které stanoví zadavatel

## IV. aktivní test fyzické bezpečnosti

- test bude dodavatelem proveden v hlavním sídle zadavatele a bude rozdělen do minimálně 2 časově rozdílných pokusů o průnik
- cíl této metody bude:
  - pokus o připojení cizího zařízení do metalické sítě zadavatele a skrze toto připojení získání přístupu do infrastruktury,
  - cílem tohoto testu není zjišťování slabých míst, jak proniknout do budovy,
  - cílem testu je otestovat odolnost metalické sítě proti nežádoucímu průniku a reakci zaměstnanců na přítomnost někoho manipulujícího s výpočetní technikou ve veřejně dostupných prostorách

## V. pasivní test fyzické bezpečnosti

- test bude dodavatelem proveden prostřednictvím vyměnitelných paměťových médií (USB flash disků) s potenciálně nebezpečným obsahem, které dodavatel doručí do 5 lokalit zadavatele, alespoň v celkovém počtu 15 ks
- testu bude předcházet dodavatelem provedená analýza cílů a metod doručení vyměnitelných paměťových médií za účelem dosažení vysoké důvěryhodnosti útoku
- zadavatel umožní připojení libovolného paměťového média – USB disku
- 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.)
- lokality určí zadavatel formou adresy a názvu organizační jednotky (oddělení/odbor) po dohodě s dodavatelem a s ohledem na provedenou analýzu cílů

## VI. test sítí

- dodavatel provede testování sítí provozovaných zadavatelem v budovách (magistrátu) zadavatele
- dodavatel provede testování bezdrátových sítí provozovaných zadavatelem a dostupných v budovách (magistrátu) zadavatele a jeho okolí (počet bezdrátových sítí: 4)
- 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.

**VII. test Active direktory**

- dodavatel provede testování Microsoft Windows domény (Active Directory, LDAP, Kerberos)
- předmětem testování bude minimálně:
  - zjistit chybné konfigurace vůči best practice Microsoftu
  - zjištění uživatelů a skupin
  - útoky na hesla
  - privilege escalation
  - kerberoasting
  - golden/silver ticket
  - pass-the-hash
  - persistence – vytvoření skrytých účtů nebo backdoorů
  - apod.
- cílem je otestovat odolnost domény, identifikovat chyby v konfiguraci a zjistit, zda lze eskalovat oprávnění od běžného uživatele k doménovému administrátorovi

**VIII. test koncových stanic**

- dodavatel provede testování vzorku koncových stanic uživatelů (min. 4)
- 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

**IX. test bezpečnosti databázových systémů**

- dodavatel provede otestování ochrany databázových serverů (operačních systémů) a samotných databází (Oracle a MSSQL) v počtu 6 databází
- Průměrný počet rolí cca 60, velikost tabulek průměrně cca 4000
- 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

**c) Požadavky na realizaci testování**

Testování bude provedeno na základě harmonogramu, který zpracuje dodavatel a schválí objednatel. V harmonogramu musí být zohledněny požadavky fázování jednotlivých testů. Dále musí harmonogram zohledňovat rozfázování jednotlivých testů tak, aby testování probíhalo alespoň 3 měsíce za účelem zvýšení důvěryhodnosti testů uživatelů a snížení podezření z jejich

strany. Doba realizace plnění je maximálně 4 měsíce od nabytí účinnosti smlouvy.

Zdroje testování budou objednatelem a dodavatelem určeny před zahájením testů a během testování budou neměnné. Změny ve zdrojích bude možné provádět pouze za účelem dosažení stanoveného scénáře, a pokud to bude nezbytné pro provedení konkrétního testu. Taková změna podléhá oznámení odpovědné osobě objednatele a jejímu schválení. Za zdroje testování objednatel považuje:

- veřejné IP adresy, ze kterých bude testování prováděno (mail servery, podvodné weby, connect servery pro škodlivý obsah, apod.)
- veřejné domény, ze kterých bude testování prováděno (mail servery, podvodné weby, connect servery pro škodlivý obsah, apod.)
- telefonní čísla, ze kterých bude testování prováděno (pro telefonní hovory i SMS),
- totožnosti osob provádějících test fyzické bezpečnosti (prokazatelná totožnost).

Dodavatel bude průběžně informovat vždy před započetím každé fáze testu a po ukončení každé fáze testu odpovědné osoby objednatele specifikované ve smlouvě.

### d) Požadavky na výstupy testů

Výstupem bude podrobná písemná zpráva ve formátu pdf obsahující zjištění, doporučení a konkrétní kroky k nápravě, doplněná o manažerské shrnutí. Zpráva musí obsahovat seznam zjištěných zranitelností, jejich dopad a hodnocení potenciálního rizika. Testovací tým poskytne informace o použitých nástrojích a technikách spolu s případnými vytvořenými skripty nebo kódem. Zpráva také bude obsahovat hodnocení zranitelností pomocí skóre a vektoru CVSS nebo CWE. Pokud je zranitelnosti přidělen CVE identifikátor, musí být uveden ve zprávě. Zpráva stanoví priority a doporučení k nápravě na základě závažnosti zranitelností a potenciálního dopadu na organizaci. Po předání závěrečné zprávy proběhne schůzka za účelem prezentace a konzultace k vysvětlení obsahu závěrečné zprávy s výsledky jednotlivých testů.

Dodavatel si ponechá všechna zdrojová data potřebná pro analýzy a testování, reprezentaci výsledků testování a sestavení průběžných i závěrečných zpráv po dobu 6 měsíců od provedené prezentace a konzultace u objednatele pro účely zodpovězení případných dotazů a otázek ze strany objednatele, popř. jeho dodavatelů.