ČASŤ 3 – Penetračný test bezpečnosti sieťovej infraštruktúry

Predmetom penetračných testov bude webové sídlo mesta Trenčín penetračné testy externej infraštruktúry v rozsahu 12 MD.

Všeobecné požiadavky na testovanie

Cieľom penetračného testovania je overenie zabezpečenia aplikácie alebo infraštruktúrnych prvkov a nájdenie slabých miest vonkajšej infraštruktúry, ktoré by mohli byť potenciálne zneužité útočníkom a mohlo by dôjsť k poškodeniu verejného obstarávateľa.

Predmetom penetračných testov je nájsť také miesta zraniteľnosti, ktorými možno prelomiť bezpečnostné opatrenia a narušiť dostupnosť, integritu alebo dôvernosť systému verejného obstarávateľa.

Napríklad:

i. získať neautorizovaný alebo neoprávnený prístup k citlivým údajom,
ii. z testovaných systémov a aplikácií vykonať neautorizované alebo neoprávnené kopírovanie citlivých dát,
iii. vykonať manipuláciu (zmenu alebo zmazanie) citlivých dát uložených v systéme, predovšetkým so zameraním na manipuláciu s informáciami o klientoch a transakciách
iv. zistiť zraniteľnosť systému a ich komponentov voči známym a relevantným typom útokov.

Výsledky testu a meraní musia byť kvantifikovateľné, opakovateľné a odvodené len na základe skutočností zistených v testoch. Všetky reportované zraniteľnosti musia obsahovať informáciu o potenciálnom riziku (závažnosti), konkrétnom postupe nápravy a informáciu o pravdepodobnosti zneužití v praxi. Všetky testy musia byť vykonávané nedeštruktívne tak, aby bolo minimalizované riziko pádu aplikácie, systému či narušenie chodu mesta.

Poskytovateľ môže podľa svojej úvahy zaradiť typy útokov na hrozby a zraniteľnosti, ktoré považuje na základe svojich skúseností alebo na základe priebežných výsledkov penetračného testovania za dôležité a relevantné pre uvedené komponenty a funkčnosti. Všetky testy budú pred samotným výkonom konzultované so verejným obstarávateľom, ktorý poskytne potrebnú súčinnosť pre prevedenie testu a poskytovateľ poskytne všetky IP a MAC adresy, z ktorých bude testovanie vykonávané.

Testovanie je možné vykonávať len v dňoch a časoch stanovených vo schválenom harmonograme a len z IP adries poskytnutých verejným obstarávateľom. Neohlásené testy z neschválených IP adries budú považované za nelegálne.

Penetračné testy webových aplikácií

Penetračné testy preveria aplikácie z pohľadu spoľahlivosti, zaistenia integrity a dôvernosti dát. Testy sú zamerané tiež na identifikáciu bezpečnostných slabín, ktoré sa môžu vyskytovať v rámci inštalácie, konfigurácie a procesov spracovania dát aplikácie.

Všetky testy sa vykonávajú bez deštruktívnych zásahov tzn., že útok končí kompromitáciou systému, nevykonávajú sa žiadne zmeny, ktoré by poškodili informačný systém.

Súčasťou testov je tiež preverenie bezpečnosti autentizačných a autorizačných mechanizmov a spôsobu zaobchádzania s citlivými informáciami v rámci testovaných aplikácií.

Penetračné testy aplikácií zahŕňajú nasledujúce kroky:

- kontrola nastavení bezpečnej komunikácie
- bezpečnosť kritických dátových tokov;
- chyby aplikácii (výpočty, náhodné chyby, strata dát);
- možnosť zneužitia aplikácii neautorizovaným spôsobom, kontrola hodnôt pri zadávaní užívateľom;
- stabilita aplikácii;

- posúdenie bezpečnostnej úrovne skriptov - nesprávne naprogramované aplikačné skripty (cgi, php, asp) môžu predstavovať bezpečnostné riziko, preto budú vybrané skripty analyzované z hľadiska bezpečnosti;
- pokus o získanie prihlasovacích údajov registrovaného užívateľa;
- náchylnosť na aplikačné zraniteľnosti definované v rámci projektu OWASP;
- bezpečnosť technológií, na ktorých sú systémy postavené (operačné systémy, webové, aplikačné a databázové servery) a ich bezpečná integrácia do ostatnej infraštruktúry;
- možnosti zneužitia dostupných technológií v aplikácii útočníkom a útoky na účty klientov.

Penetračné testy externej infraštruktúry

Cieľom externých penetračných testov je overenie odolnosti vonkajšieho perimetra spočívajúce najmä v odolnosti aktívnych zariadení ako napr.. webových, poštových, DB serverov, firewallov, aktívnych prvkov apod.
V rámci týchto testov predpokladáme:
Testovanie bude prebiehať primárne formou „black-box" a podľa metodológie OSSTMM, PTES.
Testovať sa budú 2 verejné IP adresy.
Je požadované použitie automatizovaných a manuálnych nástrojov pre testovanie, pričom manuálny prístup musí na zákazke vždy prevládať. Hlavnou prioritou je identifikovať vysoko rizikové zraniteľnosti, ďalej identifikovať také kombinácie zraniteľností nižšieho rizika, ktoré zneužitím v konkrétnej sekvencii tvorí vysoko rizikovú zraniteľnosť.
Verejný obstarávateľ k prevedeniu penetračných testov poskytne nevyhnutnú súčinnosť pre ich realizáciu.
K prenikaniu do systémov nie je u tejto služby dovolené používať sociálne inžinierstvo, okrem konkrétnych prípadov požadovaných zadávateľom a špecifikovaných v objednávke.
Priebeh realizácie testov

1. Objednávateľ špecifikuje, ktoré systémy či infraštruktúrne prvky budú predmetom penetračného testovania.
2. Poskytovateľ predloží k odsúhlaseniu harmonogram testov vrátane informácií o súčinnosti zo strany Objednávateľa.
3. Poskytovateľ vykoná testy z pozície útočníka z internetu.
4. Poskytovateľ vypracuje správu o priebehu a výsledkoch testov podľa záväznej štruktúry.

Záverečná správa

Výstupom všetkých penetračných testov je záverečná správa, ktorá popisuje podrobnosti o priebehu testu, popis a klasifikácii nájdených zraniteľností vrátane doporučení ku zníženiu zisteného rizika.
Záväzné náležitosti záverečnej správy:

1. Názov testovaného systému alebo aplikácie;
2. Manažérske zhrnutie obsahujúce tabuľku s nálezmi vrátane:
   - Popis nálezu,
   - Dopad zraniteľnosti,
   - Závažnosť (severity) nálezu,
   - Odporučenie k odstráneniu alebo zmiernenie nálezu,
   - Odkaz na príslušnú kapitolu s detailným popisom nálezu.
3. Použitá metodika testovania vrátane spôsobu klasifikácie zraniteľností.
4. Zoznam nájdených zraniteľností rozdelený do kategórií podľa metodiky CVSS verzie 3.0, resp. PTES pro Red Team testy radených podľa závažnosti od najzávažnejšej po najmenej závažnú.
5. Návrh adekvátnych riešení k odstráneniu alebo zmierneniu nálezov.
6. Konkrétny vzorový príklad úspešného útoku ku každej nájdenej zraniteľnosti (len u stredného a vysokého stupňa rizika podľa CVSS, resp. PTES).

Minimálne požiadavky verejného obstarávateľa na predmet zákazky:

Penetračný test bezpečnosti sieťovej infraštruktúry

Navrhovaná cena uchádzača			
Názov aktivity	**Názov výdavku**	**MJ**	**Počet MJ**
Analýza a dizajn	IT analytik	ČD	1
	Špecialista pre bezpečnosť IT	ČD	1
Implementácia a testovanie	IT programátor/vývojár	ČD	1
	IT analytik	ČD	3
	Špecialista pre infraštruktúrny/HW špecialista	ČD	2
	IT/IS konzultant	ČD	2
Nasadenie	Špecialista pre infraštruktúrny/HW špecialista	ČD	1
	IT/IS konzultant	ČD	1

Príloha č. 2: Doba plnenia Služby, časový harmonogram

ČASŤ 3 - Penetračný test bezpečnosti sieťovej infraštruktúry

Harmonogram realizácie projektu:

Časť 3	počet týždňov				spolu týždňov
Analýza a dizajn	4				**4**
Implementácia a testovanie			8		**8**
Nasadenie				4	**4**
Nákup technických prostriedkov, programových prostriedkov a služieb		2			**2**

Príloha č. 3 – Položkovitý rozpočet a návrh riešenia Poskytovateľa

Položkovitý rozpočet

Predmet zákazky: Zvýšenie úrovne informačnej a kybernetickej bezpečnosti mesta Trenčín

Časť 3 **Penetračný test bezpečnosti sieťovej infraštruktúry**

Penetračný test bezpečnosti sieťovej infraštruktúry

Navrhovaná cena uchádzača					
Názov aktivity	**Názov výdavku**	**MJ**	**Jednotková cena bez DPH v EUR**	**Počet MJ**	**Cena spolu bez DPH v EUR**
Analýza a dizajn	IT analytik	ČD	550,00 €	1	550,00 €
	Špecialista pre bezpečnosť IT	ČD	550,00 €	1	550,00 €
Implementácia a testovanie	IT programátor/vývojár	ČD	550,00 €	1	550,00 €
	IT analytik	ČD	550,00 €	3	1 650,00 €
	Špecialista pre infraštruktúrny/HW špecialista	ČD	550,00 €	2	1 100,00 €
	IT/IS konzultant	ČD	550,00 €	2	1 100,00 €
Nasadenie	Špecialista pre infraštruktúrny/HW špecialista	ČD	550,00 €	1	550,00 €
	IT/IS konzultant	ČD	550,00 €	1	550,00 €
				SPOLU	**6 600,00 €**

Príloha č. 4: Zoznam subdodávateľov

ZOZNAM SUBDODÁVATEĽOV

Uchádzač: AUTOCONT s.r.o., so sídlom Krasovského 14, 851 01 Bratislava, IČO: 36396222, týmto vyhlasujem, že v nadlimitnej zákazke na dodávku tovaru - predmet zákazky:

Zvýšenie úrovne informačnej a kybernetickej bezpečnosti mesta Trenčín: časť 3 - Penetračný test bezpečnosti sieťovej infraštruktúry

- ~~**nebudem využívať subdodávky a celé plnenie zabezpečím sám (tým nie je vylúčená neskoršia možnosť zmeny, avšak za splnenia pravidiel zmenu subdodávateľov počas plnenia zmluvy, ktoré sú uvedené v súťažných podkladov)**~~
- **budem využívať subdodávky a na tento účel uvádzam:**

Podiel zákazky, ktorý mám v úmysle zadať tretím osobám:

42%, t. z. 2 750,00 € bez DPH

- navrhovaní subdodávatelia

Obchodné meno	Sídlo	IČO	Kontaktná osoba
AUTOCONT a.s.	Hornopolní 3322/34,Moravská Ostrava 702 00 Ostrava Česká republika	043 08 697	**Ondej Matuštík** 18.08.1982 č.p. 749, 696 71 Blatnice pod Svatým Antonínkem **Tomáš Ječmínek** 27.03.1979 Zálužická 159/2, Cholupice, 143 00 Praha 4

- predmety subdodávok:

Obchodné meno subdodávateľa	Predmet subdodávky	Výška subdodávky (v %)	Výška subdodávky (v €)
AUTOCONT a.s.	Analýza a dizajn (IT analytik, Špecialista pre bezpečnosť IT), Implementácia a testovanie (IT analytik)	42%	2 750,00 €

- Vyhlasujem, že navrhovaný subdodávateľ spĺňa alebo najneskôr v čase plnenia bude spĺňať podmienky účasti týkajúce sa osobného postavenia a neexistovali u neho dôvody na vylúčenie podľa § 40 ods. 6 písm. a) až h) a ods. 7 zákona; oprávnenie dodávať tovar, uskutočňovať stavebné práce alebo poskytovať službu sa preukazuje vo vzťahu k tej časti predmetu zákazky, ktorý má subdodávateľ plniť.

Príloha č. 5: Zoznam osôb zodpovedných za poskytnutie služby

Zoznam osôb (expertov) ČASŤ 3 - Penetračný test bezpečnosti sieťovej infraštruktúry

Expert č.	Odbornosť experta (oblasť požadovaných znalostí)	Meno experta	Kvalifikácia experta (názov certifikátu)	Zamestnávateľ
1.	IT programátor/vývojár	Matúš Čorný	X	AUTOCONT s.r.o.
2.	Špecialista pre bezpečnosť IT	Luděk Mandok	CISA	AUTOCONT a.s.
3.	Špecialista pre infraštruktúry/HW špecialista	Jozef Burák	CCNP Enterprise	AUTOCONT s.r.o.
4.	IT analytik	Ján Pastyřík	CompTIA Security+	AUTOCONT a.s.
5.	IT konzultant	Daniel Danaj	X	AUTOCONT s.r.o.