TAYLOR McCOY

Nabídka na:

IT Bezpečnostní test

Vypracovaná pro:

Město Stod

Předkládá:

Taylor McCoy s.r.o.

Bratislavská 1487/7

102 00 Praha 10

Vypracoval:

Ing. Michal Zábelka

Email: [redacted]

Tel. +420 [redacted]

Obsah

1. Představení společnosti

1.1. Identifikační údaje dodavatele

Obchodní jméno	**Taylor McCoy s.r.o.**
Právní forma	společnost s ručením omezeným
Rok založení	2013
Sídlo společnosti	Bratislavská 1487/7, 102 00 Praha 10
Seznam statutárních zástupců	Lucie Zábelková, BA, jednatel
Kontaktní údaje	Tel.: +420 [redacted] www.tmcoy.cz
IČ	01865340
DIČ	CZ01865340
Zápis v OR	Společnost je zapsána v Obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 212710
Bankovní spojení	Raiffeisen Bank
Číslo účtu	7394093001 / 5500
Zástupce v tomto jednání	Ing. Michal Zábelka Mobil: +420 [redacted] e-mail: [redacted]

1.2. Informace o společnosti Taylor McCoy

Taylor McCoy s.r.o. je poradenská společnost poskytující odborné know-how v oblastech bezpečnosti informací. Komplexní a systémový postup našich konzultantů je jasnou a přímou cestou k dosažení požadované úrovně bezpečnosti informací a informačních systémů našich klientů.

Společnost Taylor McCoy se specializuje na poskytování služeb vysoce odborných specialistů schopných prokázat se všemi významnými profesními certifikacemi, jako jsou CISSP, CISM, CISA, ISSMP, Resilia, ITIL, Lead Auditor dle standardů ISO/IEC 20000, ISO/IEC 27000 a ISO 9001. Naši konzultanti jsou členy sdružení ISACA a itSMF Czech Republic (**www.itsmf.cz**), zároveň autory a lektory ISMS, ITIL/ITSMS kurzů.

Specialisté a konzultanti společnosti Taylor McCoy jsou připraveni vám pomoci v následujících oblastech:

- Analyzujeme rizika související s provozem nebo změnou IT prostředí a doporučíme, jak snížit rizikové faktory
- Pomůžeme Vám dosáhnout souladu s požadavky standardů a norem:
  - ISO 27001, ISO 20000
  - PCI DSS
  - Zákona o kybernetické bezpečnosti č. 181/2014 Sb.
  - GDPR
- Vytvoříme pro vás bezpečnostní politiky a procedury a vyškolíme na ně vaše zaměstnance
- Provedeme hodnocení a návrh bezpečnosti architektury
- Provedeme audity
  - systému řízení bezpečnosti podle ISO/IEC 27001
  - systému řízení IT služeb / ITIL podle ISO/IEC 20000-1
  - systému řízení kvality podle ISO 9001
- Připravíme či posoudíme vaše havarijní plány, nastavíme postupy zvládání mimořádných událostí a pomůžeme vám s plánováním kontinuity provozu
- Připravíme vás na získání certifikátů ISO 27000, ISO 20000
- Pomůžeme vybudovat a dlouhodobě udržovat bezpečnostní povědomí u vašich zaměstnanců

Námi realizované služby jsou vždy přizpůsobeny individuálním potřebám klienta a jsou v souladu s mezinárodními normami, příslušnou legislativou a dobrou vžitou praxí.

2. Cíl a rozsah testu

Předmětem dodávaného díla je provedení bezpečnostního testu vybraných informačních systémů a souvisejícící IT infrastruktury Města Stod, v následujícím rozsahu:

- serverová fyzická infrastruktura
- síťová infrastruktura
- a nad nimi provozovanými informačními systémy:
    - IS01 – AthenA (PilsCom, s.r.o.) = elektronická spisová služba + modul Smlouvy
    - IS02 – Avensio (Alfa Software s.r.o.) = personální systém
    - IS03 – Helios Fenix (Asseco Solutions a.s.) = agendový IS
    - IS04 – ESPI 8 (INISOFT s.r.o.) = evidence správních řízení
    - IS04 – EVI (INISOFT s.r.o.) = životní prostředí, agenda ovzduší
    - IS05 – Stavební a vodoprávní (VITA software s.r.o.) = stavební a vodoprávní úřad
    - IS06 – Portál úředníka = MS SharePoint 2013 Foundation

Bezpečnostní test bude realizován z pohledu útočníka, který má přístup do vnitřní sítě Města Stod na úrovni uživatele uvedených informačních systémů. Pokud některý z uvedených informačních systémů je dostupný z vnější sítě Internet bude bezpečnostní test zahrnovat i simulaci chování útočníka bez přístupu do vnitřní sítě Města Stod bez uživatelských privilegií.

Vzhledem k tomu, že bezpečnostní test bude prováděn v produkčním prostředí, během realizaci bezpečnostního testu budou použité způsoby testování omezeny na ty, které minimalizují negativní dopad na testované informační systémy a související infrastruktury

3. Popis postupu provedení bezpečnostního testu

Během provádění bezpečnostního testu vycházíme s metodik PTES (Penetration Testing Execution Standard), NIST 800-115 Technical Guide to Information Security Testing and Assesment a OWASP (The Open Web Application Security Project), jejímiž součástmi jsou následující činnosti:

- identifikovat zranitelnosti testovaných systémů,
- zjistit důsledky nalezených zranitelností na selhání testovaných systémů,
- doporučení oprav zjištěných zranitelností testovaných systémů.

Samotný bezpečnostní test se sestává z několika na sebe navazujících činností, které lze rozdělit do následujích fází:

- **Sběr informací** – sběr informací o aplikacích a prostředí, ve kterém jsou provozovány zahrnující
    - detekci zařízení, která se nacházejí na testovaném rozsahu IP adres;

- identifikace typu zařízení a provozovaných služeb;
- volba testovací strategie pro zjištěné servery, síťové prvky a webové a jiné aplikace v závislosti na využívaných technologiích apod.

- **Testování zranitelností síťové infrastruktury –** provedení testů síťové infrastruktury zahrnující
  - testy na známé zranitelnosti publikované v databázi CVE včetně konkrétních útoků na síťové prvky.
  - test ARP poisoning a odposlechu komunikace mezi různými zařízeními v síti.
- **Testování zranitelností fyzické a virtuální serverové infrastruktury** – provedení testů na známé zranitelnosti publikované v databázi CVE včetně konkrétních útoků na servery.
- **Testování aplikací** – zjištění možných zranitelností za použití automatizovaných skenů zranitelností s využitím specializovaných nástrojů s využitím specializovaných nástrojů a ručního ověření, a to v roli neautentizovaného uživatele. Obsahem jsou následující činnosti:
  - testování konfigurace, např. otestování známých bezpečnostních zranitelností zastaralých aplikačních verzí, případně nalezení chyb v konfiguraci, které by mohly být zneužity.
  - testování vůči výchozím uživatelským účtům, testování nejčastěji užívaných uživatelských jmen a hesel, enumerace uživatelských účtů. V tomto kroku budou využita také uživatelská jména získaná v průběhu sběru informací;
  - testování eskalace uživatelských práv a získání neoprávněného přístupu k informacím;
  - testování autentizace zahrnující ochranu autentizačních informací před zneužitím, správu uživatelů a hesel a možnosti útoků na použité autentizační mechanismy;
  - testování řízení relace, např. analýza HTTP relace a dalšího zabezpečení na straně klienta.

Pro dodavatele je velmi důležité držet vysoký standard v oblasti bezpečnostních testů. Z tohoto důvodu testeři dodržují tyto principy:

- včasné hlášení a upozorňování na problémy
- jasné a konzistentní závěrečné zprávy
- i při provádění detailních testů je udržován „velký obrázek“
- kreativita a efektivita šetří klientům peníze
- testy musí být metodické a opakovatelné

3.1. Používané nástroje

Všechny používané nástroje splňují několik základních kritérií, které obecně zajišťují vyšší bezpečnost a důvěryhodnost prováděných testů a omezují rizika vznikající při testování produkčních systémů.

- Všechny nástroje jsou důkladně testovány na vlastním polygonu s cílem ověřit jejich správné fungování, skutečně vykonávané funkce a možné dopady na testované i okolní části systému.
- Všechny klíčové nástroje jsou analyzovány a kompilovány pracovníky dodavatele. Nástroje, u kterého toto není možné, jsou zvýšenou měrou testovány a používají se pouze pro detekční účely, a ne ve fázích vytváření nebo udržování přístupu do testovaného systému.
- V případě potřeby použití speciálního kódu na využití existující slabiny (tzv. exploit) jsou vždy preferovány vlastní programy nebo ty, u kterých je možné provést kontrolu zdrojového kódu a otestovat jejich funkčnost na polygonu.

Většina uvedených nástrojů nemá žádný, nebo jen minimální škodlivý dopad na vlastní testované systémy. U nástrojů, kde existuje vyšší riziko, ale kde kvalita a přidaná hodnota nástroje nelze nahradit žádným bezpečnějším způsobem, je toto uvedeno. Použití těchto nástrojů je vždy plánováno na dobu, ve které nejsou produkční systémy příliš využívány.

4. Výstupy z testu

Výstupem bezpečnostních testů bude výsledná souhrnná závěrečná zpráva obsahující cíl a rozsah testů, zhodnocení odhalených bezpečnostních nedostatků podle stupně jejich závažnosti a doporučení na nejvhodnější způsob jejich odstranění či maximální snížení rizika zneužití.

5. Organizace projektu a součinnost Zadavatele

Ze strany zadavatele je nezbytné určení jedné kontaktní osoby, která bude pro tým zpracovatele partnerem pro veškerou oficiální komunikaci a bude mít pravomoc schvalování veškerých potřebných kroků pro úspěšné dovršení projektu v zadaném čase. Odpovědná osoba bude informována o všech prováděných aktivitách. Kontaktní osoba bude dále zodpovědná za zajištění všech potřebných kroků ze strany zadavatele, zejména obstarání požadované dokumentace, plánování schůzek, akceptaci výstupů apod.

Vzhledem k ochraně důvěrných informací spolu obě strany dohodnou způsob zabezpečení vzájemné elektronické komunikace (symetrické šifrování, digitální certifikáty apod.). Komunikace bude probíhat v českém jazyce.

V průběhu realizace mohou být požadavky na součinnost rozšířeny dle aktuálních potřeb. V takovém případě bude součinnost vyžádána vždy v předstihu.

Mezi další možné požadavky na součinnost patří:

- Poskytnutí související dokumentace (topologie sítě)
- Zajištění přístupu do prostor Zadavatele po dobu trvání projektu
- Zajištění uživatelského přístupu do testovaných informačních systémů a související infrastruktury
- Poskytnutí pracovního místa, vybaveného s připojením do testovaných síťových segmentů dle rozsahu požadovaného testu po dobu trvání projektu
- Poskytnutí součinnosti s připojením zařízení pro hloubkovou analýzu síťové prostředí
- Zřízení vzdáleného přístupu do prostředí objednatele

6. Cenová nabídka

Společnost Taylor McCoy si Vám dovoluje předložit nabídkovou cenu v návaznosti na poptávané činnosti.

	Popis	*Cena bez DPH*	*Cena včetně DPH*
1.	Cena za služby „IT bezpečnostní test“	100 000,-	121 000,-
Celkem		**100 000,-**	**121 000,-**

Všechny ceny jsou uvedeny bez DPH v českých korunách (CZK) a zahrnují veškeré náklady uchazeče spojené s vypracováním analýzy.

7. Závěr

Všichni pracovníci společnosti Taylor McCoy, kteří se podíleli na přípravě této nabídky, tak činili s maximálním úsilím a odbornou znalostí ve snaze maximálně a úplně reagovat na požadavky Zadavatele. Věříme, že Vás naše nabídka a návrh v ní obsažený zaujme a budeme pro vás kvalitními partnery.

Děkujeme Vám za čas, který jste věnovali prostudování naší nabídky. V případě doplňujících dotazů se na nás můžete kdykoliv obrátit. Po vzájemné dohodě jsme připraveni Vás znovu navštívit, poskytnout Vám další informace a pokračovat v zahájených jednáních, které doufáme, povedou k Vaší plné spokojenosti.

Doufáme, že naše nabídka splní Vaše očekávání a bude se tak moci stát základním kamenem našeho budoucího partnerství na poli informační bezpečnosti.