VIAVIS střežíme podstatné

Penetrační testy systému SOBD

pro „Magistrát města Brna“

27. duben 2021

VIAVIS a. s. | Obránců míru 237/35 | 703 00 Ostrava | [redacted]

zapsána v obchodním rejstříku vedeném Krajským soudem v Ostravě | Oddíl B, číslo vložky 2249 | IČ 25848402 | DIČ CZ25848402

VIAVIS střežíme podstatné

ZÁKLADNÍ ÚDAJE O SPOLEČNOSTI

Obchodní firma	**VIAVIS a.s.**
Sídlo společnosti	Obránců míru 237/35, 703 00 Ostrava-Vítkovice
Společnost je zapsána	v obchodním rejstříku, Krajský soud v Ostravě, spis B 2249
IČ	25848402
DIČ	CZ25848402
Bankovní spojení	[redacted]
Číslo účtu	
Telefon	
ID datové schránky	
E-mail	
URL	

Obsah

1 Manažerské shrnutí

Společnost VIAVIS a.s. si váží vašeho zájmu o vypracování této nabídky. Při jednání bylo dohodnuto, že předložíme nabídku na provedení penetračního testu ICT systému – testu odolnosti bezpečnostních mechanismů.

Děkujeme za čas, který věnujete naší nabídce. Věříme, že reflektuje na vaše potřeby a splňuje vaše požadavky na realizaci tohoto projektu.

Děkujeme za vaši přízeň a doufáme, že vás naše nabídka zaujme.

S pozdravem

[redacted]

2 Předmět nabídky

Předmětem této nabídky je provedení penetračních testů neboli testů odolnosti bezpečnostních mechanismů, procesů, případně rizikovosti chování zaměstnanců simulací reálného bezpečnostního incidentu. Cílem těchto testů je ověřit zabezpečení a identifikovat zranitelnosti **IS SOBD**.

2.1 Popis testování

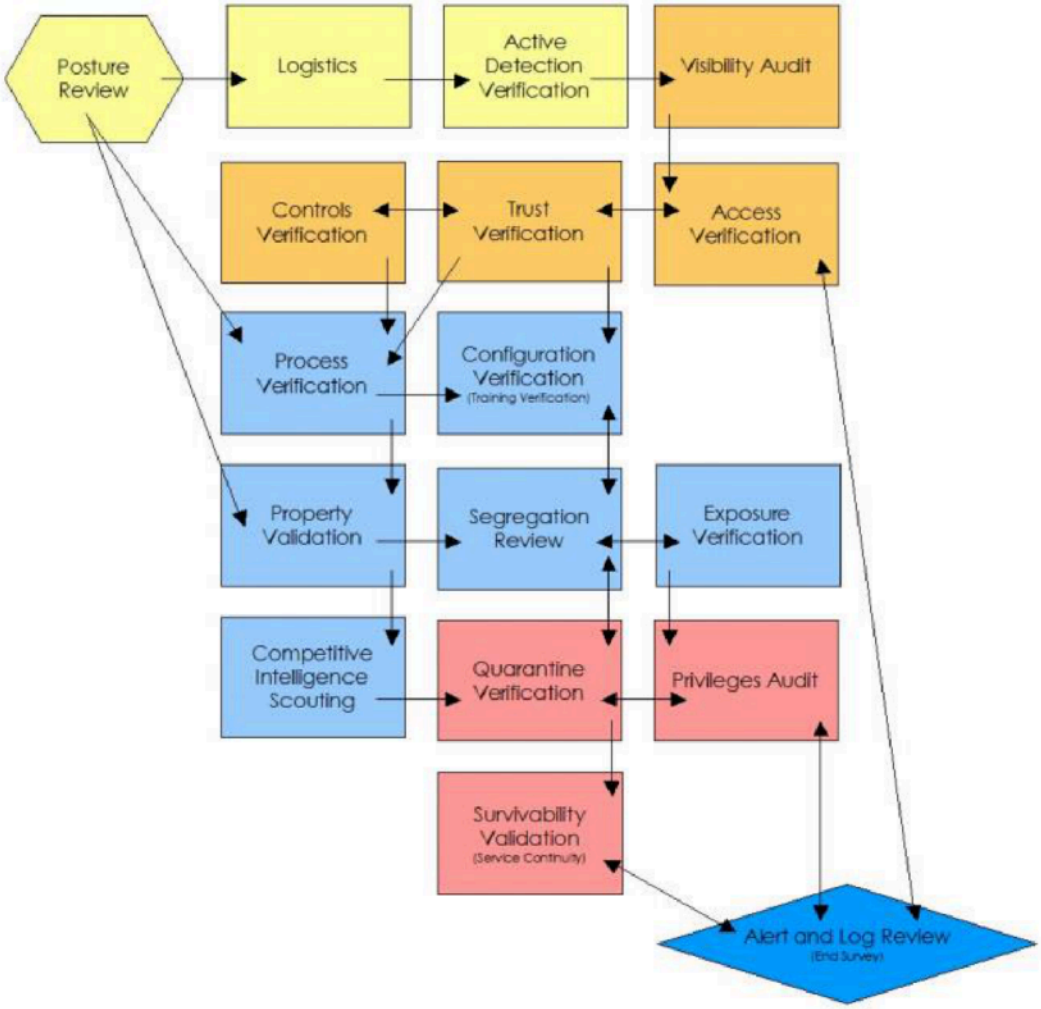
Penetrační testování bude provádět dle metodiky **OSSTMM** (Open Source Security Testing Manual) a metodiky **OWASP** (Open Web Application Security Project) a **ISACA** guidelines.

OSSTMM stanovuje základní principy a pravidla, která určují (vymezují) co se bude, jak a kdy testovat a rozděluje potřebné úkoly, které musí být provedeny. Spojením všech jednotlivých modulů metodiky získáme procesní mapu jednoduše zobrazující aplikaci samotné metodiky.

Z pohledu procesní mapy je tato rozdělena na několik jednoduše odlišitelných fází:

- úvodní fáze;
- fáze interakce;
- fáze vyšetřování;
- nápravná fáze.

Na následujícím obrázku je zobrazena mapa průchodu jednotlivými moduly. Cestu si volí, dle specifikace standardu, obvykle testující konzultant sám.



Aplikace metodiky nebude lineární, jak je zřetelné z vazeb mezi jednotlivými moduly. Tato situace znamená, že samotný průchod (konkrétní cestu) mezi moduly bude vybírat testující konzultant sám, a předpokládá se i zpětný postup a tím využití znalostí získaných během aplikace „pozdějších“ modulů.

Způsob aplikace metodiky:

Vlastní testování probíhá dle schválených testovacích scénářů a v době, která je zadavatelem dopředu odsouhlasena.

V případě, kdy během testu je odhalena zásadní bezpečnostní slabina, je odpovědná osoba o této skutečnosti informována ihned, a to včetně návrhu na rychlé řešení eliminace této slabiny.

2.2 Interní penetrační test

Interní penetrační testy budou prováděny z prostředí interní LAN sítě zadavatele. Jejich cílem je prověření bezpečnosti systému v rámci jeho provozního prostředí a provozu interní sítě, kde se dá předpokládat nižší úroveň zabezpečení.

Bude tedy proveden řízený útok na infrastrukturu zadavatele z vnitřní sítě, tj. bude simulováno počínání potencionálního útočníka pokoušejícího se o průnik z vnitřní sítě.

Interní penetrační testy budou částečně kopírovat externí testy pro interní datovou síť a dále budou zaměřeny na:

- Testů k získání informací, identifikace funkčních systémů;
- všeobecných testů zranitelnosti;
- testů týkajících se charakteristiky infrastruktury systému;
- testů spolehlivosti konfigurace;
- testů existence backdoors;
- testů autentizace a schémat pro kontrolu přístupu;
- kontroly operačních systémů;
- testů aplikačních chyb a vad v systému;
- testů nedostatečného provozního zabezpečení;
- testování slabých míst zahrnující body selhání, s cílem způsobit odmítnutí služeb webových aplikací;
- odposlech komunikace se systémem;
- odchycení a přesměrování této komunikace;
- zneužití odchycených informací a komunikace směrem k aplikačním službám (serverům);
- útoky na uživatele systému prostřednictvím tohoto systému;
- testů wi-fi bodů přístupu.

2.3 Přípravná etapa

Souhlas zadavatele s testovacími scénáři a časem testování je nezbytný, protože při penetračním testu nelze vyloučit výpadek či nedostupnost bezpečnostních mechanismů. Proto musí být testováno v době, kdy je riziko vzniku jakýchkoli problémů minimální a lze zorganizovat jejich případné řešení.

Je poté nutné rozhodnout o jaký typ testu se bude jednat:

1. Nekooperativní testy bez znalosti na straně provozovatele – tedy provozovatel/správce systému o realizaci testů neví – dojde tedy nejen k testování IS SOBD, ale i k testování proaktivních mechanismů systémů a správy. Jako vlastník systému máte tzv. právo auditu, čili je možné takto postupovat. Jen může při zachycení útoku na straně provozovatele dojít k blokaci sítě MMB a je

tedy možné řešit kompromisní řešení, kdy o testování ví vrcholový pracovník provozovatele/správce – není to ale nutné.

2. Nekooperativní testy se znalostí na straně provozovatele – provozovatel/správce bude plně informován o realizaci testování. Zde bude předejito případným eskalacím „bezpečnostního incidentu“, nejedná se ale o standardní operační prostředí.

2.4 Vlastní testování

Vlastní testování probíhá dle schválených testovacích scénářů a v době, která je zadavatelem dopředu odsouhlasena.

Testující konzultanti VIAVIS dokumentují veškeré své činnosti, které při testování provádějí, dokumentují dále veškeré zaznamenané reakce bezpečnostních mechanismů a zaměstnanců, včetně informaci o čase a dostatečnosti reakce.

V případě, kdy během testu je odhalena zásadní bezpečnostní slabina, je odpovědná osoba o této skutečnosti informována ihned, a to včetně návrhu na rychlé řešení eliminace této slabiny.

2.5 Výstup z testování

Výstupem penetračních testů bude písemná zpráva „Závěrečná zpráva z penetračních testů“ o stavu bezpečnosti jednotlivých prověřovaných oblastí s popisem bezpečnostních opatření, která jsou doporučena pro odstranění nalezených problémů.

Ve zprávě bude obsažen zejména detailní postup provedených penetračních testů, včetně použitých nástrojů, technik, reakcí zaměstnanců objednatele a výsledek testování. Výsledkem je tedy aktuální informace o stavu systémů a prakticky se ověří nastavení bezpečnostní politiky.

2.6 Cenová nabídka

Popis	**MD**	
Interní penetrační testy včetně závěrečné zprávy	7 MD	84.000,- Kč bez DPH

3 Profil společnosti VIAVIS a.s.

VIAVIS a.s. je znalostní a konzultační společnost orientující sena poskytování nezávislých a vysoce odborných služeb v oblasti ochrany a bezpečnosti informací, projektového a procesního managementu a řízení ICT služeb. Na trhu působí VIAVIS a.s. od roku 1999 a mezi jeho stálé zákazníky patří řada významných společnosti v České republice i zahraničí.

Tým konzultantů a lektorů **VIAVIS a.s.** se skládá ze špičkových odborníků na ICT a informační bezpečnost, na problematiku fyzické, personální a administrativní bezpečnosti. Svou odbornost dokládají získanými certifikáty, členstvím v prestižních odborných asociacích a kvalifikací soudního znalce. Protože jsme si vědomi společenské odpovědnosti, konzultanti **VIAVIS a.s.** se aktivně zapojují do výuky na vysokých školách, kde přednáší například o problematice kybernetické bezpečnosti či vedou diplomové práce. Základními hodnotami, na kterých stavíme spolupráci s našimi zákazníky, jsou důvěryhodnost, diskrétnost, etika a profesionalita.

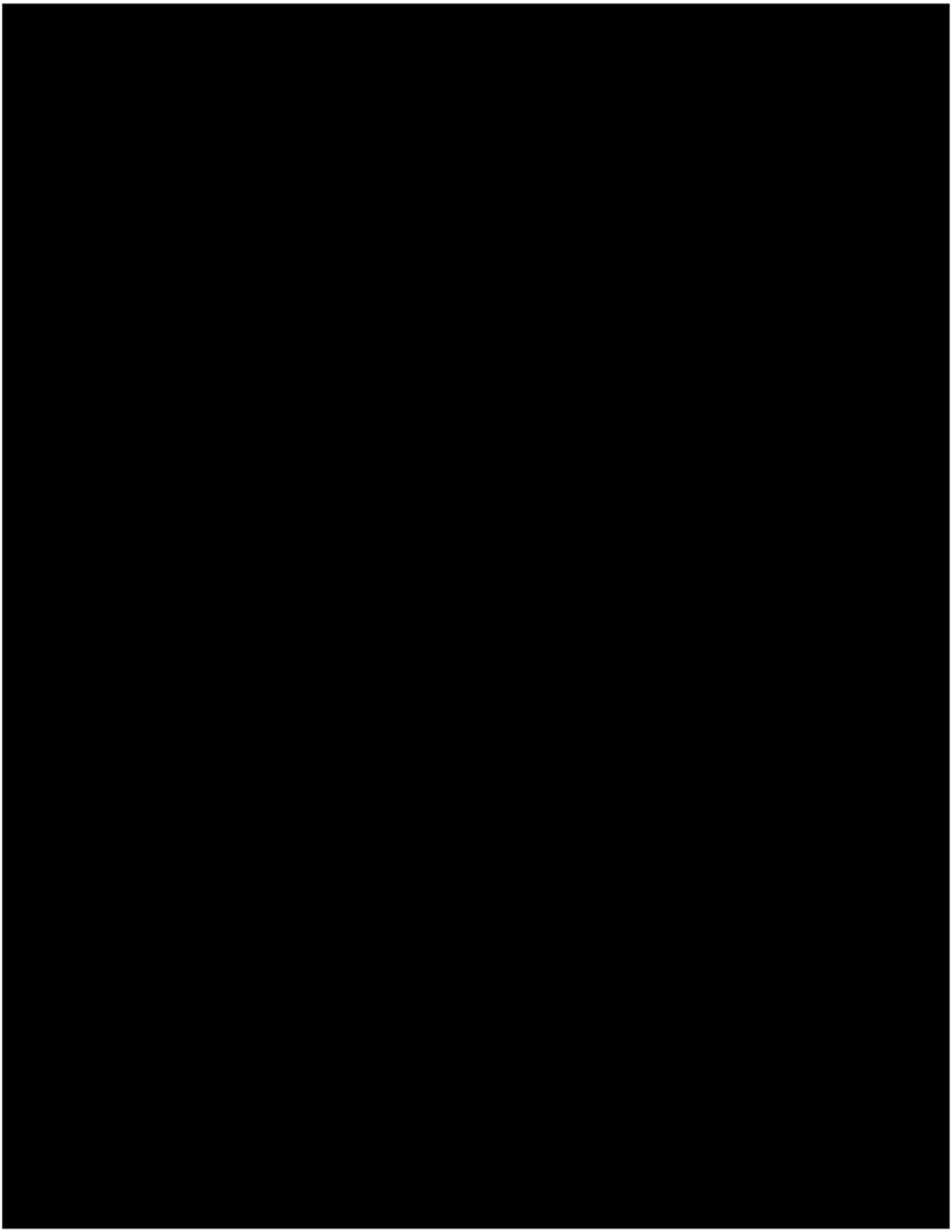
3.1 Divize informační bezpečnost

- audity, posouzení stavu bezpečnosti informací, ochrana obchodního tajemství, know how;
- penetrační testy, řešení bezpečnostních incidentů, provozní outsourcing bezpečnosti systémů infrastruktury IS;
- projekty v oblasti fyzické ochrany osob, majetku a informací, vč. projektů ochrany měkkých cílů
- zavedení systému řízení bezpečnosti informací – ISMS (Information Security Management System) a jeho příprava k certifikaci dle ISO/IEC 27001 (www.isms.cz);
- řízení informačních rizik – analýza rizik, zvládání rizik, návrhy protiopatření, integrovaná ochrana informací;
- ochrana osobních údajů dle obecného nařízení o ochraně osobních údajů (GDPR) a zákona č. 110/2019 Sb., o zpracování osobních údajů;
- RANIT – vlastní software pro podporu řízení rizik (www.ranit.cz);
- speciální projekty pro sektor financí – řízení operačního rizika bank a finančních institucí, naplnění požadavků regulace ČNB v oblasti ochrany informací;

3.1.1 Certifikace/bezpečnostní dovednosti

Ve firmě působí dva soudní znalci v oboru Kybernetika.

K předmětné aktivitě disponují naši zaměstnanci certifikáty CISA (certified information systems auditor) a CEH (certified ethical hacker).



3.2 Divize konzultací

- Komplexní poradenství při výběrových řízeních informačních systému (organizace výběrového řízení, hodnocení nabídek, doporučení vhodného systému a sjednání smluv) a při následných implementacích (odborný dohled při nasazení informačních systémů – řízení projektu na straně implementujícího, audit implementačních projektů, mediace problémových projektů);
- Analýzy procesů a jejich optimalizace, auditní činnost, vypracování znaleckých posudků

3.3 Divize vzdělávání

- Organizace seminářů a vzdělávání pro široké spektrum klientů - jednotlivce, veřejnou a státní správu, malé firmy i korporace
- VIAVIS a.s. byla udělena akreditace Ministerstva vnitra ČR pro oblast průběžného vzdělávání úředníků a vedoucích úředníků
- VIAVIS a.s. byla akreditována také u Ministerstva školství, mládeže a tělovýchovy ČR jako vzdělávací instituce v systému DVPP (Další vzdělávání pedagogických pracovníků)

3.4 Reference

Konzultace