DCIT

Nabídka: Penetrační test internetového bankovnictví

NABÍDKA

Zhotovitel:	**DCIT, a.s.** Kodaňská 1441/46 101 00 Praha 10 https://www.dcit.cz
Adresát:	**Českomoravská záruční a rozvojová banka, a.s.**
Poptávka:	06.10.2020 [redacted]
Ve věci nabídky je oprávněn jednat:	[redacted]
Datum vyhotovení:	15.10.2020
Platnost nabídky:	31.12.2020
Počet stran:	11

DCIT

Obsah

1 Úvod

Úvodem dovolte vyslovit poděkování za možnost podání nabídky našich služeb. Pevně věříme, že Vás nabídka zaujme a že společně navážeme oboustranně prospěšnou spolupráci, při které budeme moci využít našich dlouholetých zkušeností.

Přehled služeb DCIT

Technická bezpečnost

Ethical hacking

- Penetrační testy WWW (OWASP)
- Penetrační testy mobilních aplikací
- Penetrační testy – API / WS
- Penetrační testy – externí
- Penetrační testy – interní
- Penetrační testy SCADA
- Penetrační testy Wi-Fi
- Zátěžové testy – DoS

Konfigurační audit

- Hardening Microsoft Windows
- Hardening UNIX
- Hardening Microsoft SQL
- Hardening Oracle DB

Ostatní

- Code review
- Školení: bezpečnost WWW aplikací
- Školení: penetrační testy

Procesní bezpečnost

Analýzy

- Analýza rizik
- Analýza dopadů (BIA)
- Analýza shody se ZoKB
- Analýza shody s ISO 27000
- Analýza shody s GDPR

Informační bezpečnost

- Implementace ISMS
- Implementace BCM
- Bezpečnostní dokumentace

Ostatní

- GDPR poradenství
- Školení: implementace ISMS
- Školení: bezpečnost pro uživatele

Více informací o nabízených službách najdete na https://www.dcit.cz/cs/sluzby

2 Předmět nabídky

2.1 Služba – Prověření WWW aplikace

Při tomto testu je simulován útok na WWW aplikaci zákazníka typicky z vnějšího prostředí, tj. **konzultant simuluje počínání potenciálního útočníka provádějícího útok z Internetu**.

Jelikož jsou **WWW aplikace** ve většině případů **softwarová díla na zakázku**, obsahují chyby, které jsou rovněž typicky neopakovatelné a „na zakázku“:

- vesměs se jedná se o specifické a **jedinečné chyby** programátora (vlastní zaměstnanec či pracovník dodavatele), které se pochopitelně neobjeví v žádné z uznávaných databází publikovaných bezpečnostních slabin;
- obvykle proto – tyto do jisté míry jedinečné problémy – **neodhalí žádný automatizovaný nástroj pro testování zranitelností** (tzv. „vulnerability scanner“) – zejména zde vyniká přínos manuálních testů a bohaté zkušenosti a kombinační schopnosti našich specialistů.

Testování WWW aplikací je zaměřeno na celou řadu **slabin specifických pouze pro tento typ aplikací** a nutně proto používá poněkud odlišné metodiky a postupy než při „standardním“ penetračním testu.

2.1.1 Typy a průběh testů

K testování webových aplikací lze přistoupit různými způsoby na základě potřeb zákazníka, způsobu používání webových aplikací a nejpravděpodobnějších scénářů útoku.

Často se lze i při penetračních testech (přestože se původem jedná o termíny pocházející z funkčního testování) setkat s označením:

- Black-box test (bez znalosti),
- White-box test (se znalostí zdrojového kódu serverové strany),
- Grey-box test (s částečnou znalostí).

Důležité je spíše rozhodnout, zda test má být **bez znalosti** či **se znalostí** (především) **autentizačních údajů** (dále AÚ).

- Testování **bez znalosti AÚ** – Prověření je prováděno z anonymní úrovně. Tato fáze testu je zaměřena na odhalení **možnosti průniku** do aplikace (a dalších souvisejících prvků, např. do databází interní sítě) **„náhodným“ útočníkem** (tzv. „outsiderem“), který nemá představu o struktuře a obsahu aplikace.
- Testování **se znalostí AÚ** – Prověření je prováděno se znalostí autentizačních a autorizačních údajů pro přístup do aplikace. Výhodou je i znalosti struktury a funkcionalit aplikace. Testy jsou nejčastěji prováděny **z úrovně běžného uživatele**. Pro účely testu proto obvykle předpokládáme přístup k 1-2 uživatelským účtům. Cílem je prověření **možnosti překročení základních práv** přidělených běžnému uživateli, neboli možnost **zneužití aplikace „řádným“ uživatelem** (tzv. „insiderem“), který má k dispozici alespoň částečnou znalost o přístupu a použití aplikace. Kromě toho je možno (za předpokladu poskytnutí alespoň 2 testovacích účtů) prozkoumat možnosti (neoprávněného) přístupu pomocí jednoho uživatelského kontextu k datům jiného uživatele, případně i provést neoprávněně transakci (obecně aplikační akci) pod jinou identitou.

Nejčastěji se kombinuje test bez znalosti autentizačních údajů (např. prověření bezpečnosti aplikace proti náhodným či automatizovaným útokům z internetu) s testem se znalostí přihlašovacích údajů, kde se prověřuje především řízení přístupu a aplikační logika.

2.1.2 Použitá metodika testování (OWASP)

Postupy používané při testování webových aplikací opíráme o neustále aktualizovanou interní metodiku, dlouhodobě vycházející z doporučení a „de-facto" standardů **OWASP** (The Open Web Application Security Project), https://www.owasp.org.

Při testování dílčích bezpečnostních aspektů aplikace postupujeme s přihlédnutím k OWASP Application Security Verification Standard (ASVS).

V rámci prověření konkrétní webové aplikace jsou pak vždy testovány pouze oblasti, které jsou relevantní dané funkcionalitě aplikace.

2.1.3 Slabiny webových aplikací

Díky množství technologií a vývojových platforem, na kterých jsou aplikace provozovány, bylo nutno stanovit dostatečně abstraktní úroveň, kterou je třeba se při hledání možných zranitelností zabývat. Dlouhodobě se touto problematikou zabývají různé organizace, v prvé řadě mezinárodní sdružení MITRE (https://cwe.mitre.org) a v současné době stále populárnější otevřené sdružení vývojářů bezpečných webových aplikací – **OWASP** (www.owasp.org), k jehož konceptům a metodikám se dlouhodobě přikláníme. Právě OWASP již po řadu let vydává seznam nejrozšířenějších slabin webových aplikací, známý jako OWASP Top10.

Okruhy nejvýznamnějších problémů WWW aplikací se sice v průběhu let (logicky s vývojem aplikací a nových útoků na ně) mírně liší, nicméně z našeho dlouhodobějšího pozorování lze vysledovat některé „stálice" – nejnebezpečnější slabiny, tj. nejrozšířenější či s nejhorším dopadem na bezpečnost aplikací, jako je injekce kódu (např. SQL injection), Cross Site Scripting (XSS) atd.

2.1.4 Nástroje používané pro testování

Při testech webových aplikací je v prvé řadě zapotřebí kombinačních schopností a zkušenosti testera, nicméně existuje množství nástrojů, které postup testování značně usnadňují a zefektivňují.

Většina nástrojů je dostupná jako „Open Source" včetně plných zdrojových kódů, je proto na místě upozornit, že mnoho z používaných nástrojů je pro účely testování v DCIT interně dopracováno a upraveno, stejně tak využíváme vlastními silami vyvinuté, proprietární nástroje pro řešení speciálních či jednorázových testovacích úloh. K tomuto účelu jsou využívány obvyklé skriptovací (Python, Perl, Ruby) a programovací jazyky (Java, C).

Testovací nástroje (včetně vlastních) využívá v úvodní fázi testování DCIT jako referenci k prvotnímu průzkumu testovaného prostředí.

Naše přidaná hodnota však spočívá zejména v následném, **manuálním a velmi podrobném šetření** možných zranitelností a jejich kontextově závislých kombinací.

Automatové nástroje mohou poskytnout předběžnou představu o základních – potenciálních zranitelnostech. **Znalosti a zkušenost technických konzultantů** však umožňuje v daném prostředí (kontextu) využít potenciálních slabin a zkombinovat je v postup, vedoucí ke kompromitaci cílového systému. Právě tato schopnost nám umožňuje s vysokou mírou přesnosti stanovovat reálnou zranitelnost testovaných systémů a našim zákazníkům přináší přesnou informaci o možných způsobech napadení jejich technologií – doplněnou o námi navržené nejvhodnější způsoby řešení těchto bezpečnostních rizik.

Díky kombinaci automatizovaných testů a manuální práce zkušených testerů DCIT dokážeme poskytnout **detailní analýzu stavu zabezpečení testovaného systému společně s podrobným popisem (záznamem) testů** tak, aby bylo možno efektivně odstranit případné problémy.

2.2 Služba – Penetrační test API / webových služeb

Specifickým, často opomíjeným, místem, ve kterém je ohrožena bezpečnost webových aplikací, je implementace API (Application Programming Interface) rozhraní, která bývají

implementována s využitím protokolu SOAP/HTTP (tzv. webové služby, webservices) nebo jako REST API. Obvykle jde o zprostředkování komunikace stroj-stroj či aplikace-aplikace. Z tohoto důvodu mu mylně nebývá věnována taková pozornost jako komunikaci uživatel-stroj/aplikace, i když dopady případných chyb mohou být fatální (únik velkého množství dat, provedení většího množství neautorizovaných transakcí).

Cílem penetračního testu API rozhraní/webových služeb je prověřit, zda je dané rozhraní bezpečné, zda pomocí něj nelze získat osobní či jiné citlivé údaje, přístup do nežádoucích oblastí nebo zda dokonce nelze cílový stroj ovládnout.

2.2.1 Varianty rozhraní

Postupy používané při testování webových služeb/API rozhraní jsou postaveny na průběžně aktualizované interní metodice, dlouhodobě vycházející z doporučení a „de-facto" standardů OWASP – The Open Web Application Security Project.

V metodice zohledňujeme zejména doporučení sdružení OWASP určená přímo pro webové služby, uveřejněná v rámci: REST Security a XML Security Cheat Sheets.

V rámci prověření konkrétního API rozhraní/webové služby jsou pak vždy testovány pouze oblasti, které jsou relevantní pro daný typ rozhraní.

Základní typy rozhraní jsou:

- Webové služby (web services) na bázi protokolu SOAP/HTTP.
- REST API rozhraní.

SOAP (Simple Object Access Protocol) je protokolem pro výměnu zpráv založených na XML přes síť, hlavně pomocí protokolu HTTP. Základním popisem SOAP rozhraní jsou WSDL definice (opět XML), které popisují jednotlivé funkce, které dané rozhraní nabízí.

REST (Representational State Transfer) je architektura rozhraní, které definuje přístup k datům pomocí 4 základních metod (CRUD – create, retrieve, update, delete), tyto metody jsou implementovány pomocí odpovídajících HTTP metod (POST, GET, PUT, DELETE). Strukturovaná data jsou v případě REST API přenášena obvykle ve formátu JSON (může být XML, ATOM aj.).

2.2.2 Průběh testování

Testování WS/REST API není na rozdíl od jiných testů vhodné realizovat přístupem black-box (bez jakýchkoliv znalostí o předmětu testu), protože tester více času stráví otázkou „Jak to funguje?", než „Kde je slabina?".

Pro efektivní testování je vhodná vzorová implementace klienta, SoapUI projekt nebo podrobná dokumentace k použitým metodám a parametrům, resp. obecně popis komunikace mezi koncovými body.

Na pracnost testování má vliv počet použitých metod, parametrů, testovacích scénářů, způsob autentizace a počet uživatelských rolí, které mají být předmětem testu.

V případě webových služeb je test realizován v následujících krocích:

Typ testu	Podrobnější popis
Základní testy	Testování standardních Request(s)/Response(s) pro každou použitou metodu.
Automatizované testy	Testování API/WS pomocí specializovaných nástrojů SoapUI a BurpSuite Professional.
Identifikace zranitelností	Důkladné testy zranitelností, zejména: Fuzzing, SQLi, Malformed XML, Malicious attachment/file upload, Xpath injection, XML bomb, Authentication based attacks, External resources, Schema implementation weaknesses, Debug output, Non-encoded output.
SOAP/JSON parser	Test parseru XML/JSON. Chování aplikace při syntaktických chybách v požadavku, popřípadě při neočekávaných jinak invalidních dotazech. Obecně slabiny na úrovni zpracování vstupů (XXE apod.).

Typ testu	Podrobnější popis
Autentizace, autorizace	Test odolnosti použité autentizační metody (Basic / SAML / OAuth / OpenID / certifikát). Možnost obcházení přístupových práv.
Parametr tampering	Manipulace s hodnotami parametrů – číselné hodnoty mimo očekávaný rozsah, vkládání neočekávaných znaků (test SQL / Xpath Injection), řetězce znaků velké délky, nekorektní formát dat oproti specifikaci.
Output encoding	Test možnosti vnutit vypsání speciálních znaků do odpovědi serveru. A to jak v samotné XML/JSON odpovědi, tak i v HTTP hlavičce. To může vést ke změně sémantiky odpovědi.
Session management	Manipulace s identifikátorem seance. Test zda je možné vnutit, podvrhnout, ukrást, nebo ovlivnit seanci. Jak se server chová na přístup k jedné seanci z různých IP.
Zátěžové testy (volitelně)	Test přítomnosti typických chyb XML/JSON parserů. Zahlcení požadavky nadměrné velikosti, příp. požadavky s vysokou komplexitou a náročností zpracování na serverové straně.

2.3 Přezkum bezpečnostních opatření

V rámci penetračního testu bude proveden přezkumu bezpečnostních opatření (metod), který je povinný pro všechny poskytovatele platebních služeb (dle regulačních technických standardů RTS SCA, klíčové součásti Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015, o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES (PSD2) (dále jen „Směrnice“).

Přezkum bude zahrnovat všechny povinné aspekty dle čl. 3 Nařízení Komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace.

V rámci přezkumu bude provedeno posouzení bankou předložených materiálů a bude provedena diskuze pracovníka DCIT s odbornými pracovníky banky z útvarů, jež mají danou problematiku ve své gesci. Zpracovaný přezkum bezpečnostních opatření bude v samostatné příloze závěrečné zprávy Penetračního testu.

2.4 Závěrečná zpráva

Výstupem penetračního testu je závěrečná zpráva, která obsahuje podrobnosti o průběhu testu, popis a klasifikaci nalezených zranitelností a samozřejmě doporučení ke snížení rizika.

Zpráva je rozdělena do následujících částí:

- **Manažerský souhrn** – stručný průřez průběhu testu společně s výsledky.
- **Popis testu** – popis metodiky testu a přehled všech prováděných činností.
- **Zjištěné skutečnosti** – detailní popis výsledků všech testů jednotlivých zařízení.
- **Shrnutí doporučení vyplývajících z testu** – přehledná tabulka doporučení, kterými lze odstranit nedostatky nalezené v průběhu testu.

Pro klasifikaci závažnosti zranitelnosti je standardně použita škála: Nízká (Low), Střední (Medium), Vysoká (High) a Kritická (Critical). V případě požadavku zákazníka přidáme hodnocení pomocí CVSS skóre nebo použijeme zákazníkem dodané klasifikační schéma.

😐	**Připomínka (LOW)** Takto jsou označovány nálezy s méně významným dopadem.
☹	**Nedostatek (MEDIUM)** Nálezy s nezanedbatelným dopadem, ale obtížně zneužitelné.
💣	**Slabina (HIGH)** Nálezy s velkým možným dopadem, vyžadující bezodkladnou opravu.
☠	**Velká slabina / průnik (CRITICAL)** Nálezy se zásadním dopadem, který byl demonstrován. Nutná okamžitá oprava.
☺	**Zlepšení / Pozitivní informace** Zlepšení oproti předchozím testům nebo dodatečná opatření zvyšující bezpečnost.

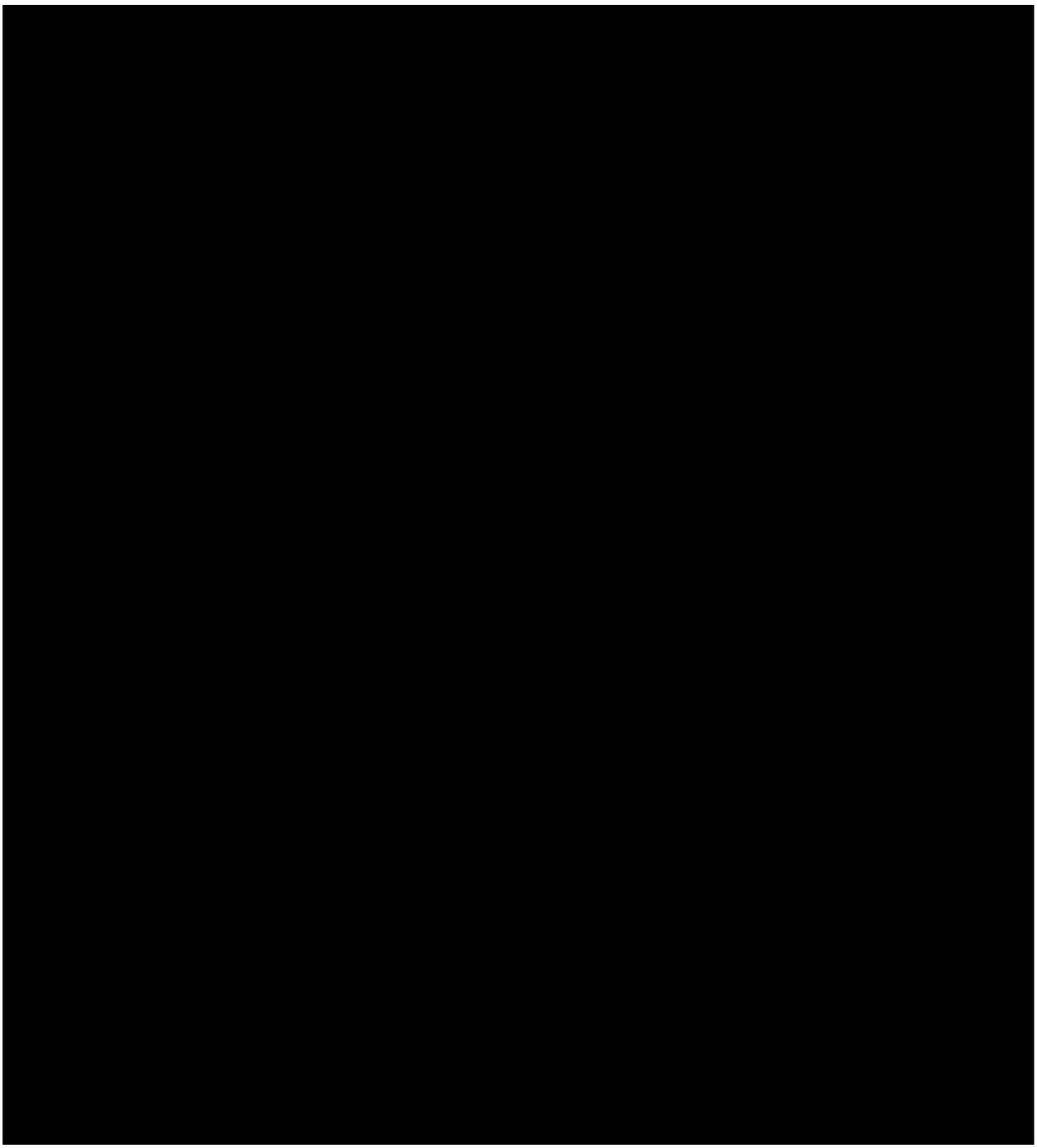
Zpráva je připravena ve formátu MS Word a PDF a zákazníkovi zaslána bezpečným způsobem.

Penetrační testy mohou být zakončeny prezentací výsledků u zákazníka – manažerská prezentace nebo technický workshop/diskuse nad závěrečnou zprávou.

2.5 CV pracovníků

[redacted]

3 Cenová kalkulace



4 Informace o DCIT, a.s.

4.1 Identifikační a kontaktní údaje

DCIT, a.s. (dále jen DCIT) je společnost působící více než 25 let v oblasti informačních technologií, která svým zákazníkům poskytuje širokou škálu komplexních služeb ve dvou hlavních oblastech, kterými jsou poradenské služby v oblasti IT a vývoj software.

jméno společnosti:	DCIT, a.s.
sídlo společnosti:	Kodaňská 1441/46, 101 00 Praha 10
statutární zástupce:	Mgr. Josef Vašica, předseda představenstva
IČ:	26143097
DIČ:	CZ26143097
zápis v OR:	Městský soud Praha, oddíl B, vložka 10075
telefon:	[redacted]
WWW:	https://www.dcit.cz/cs

4.2 Kvalifikační předpoklady

Společnost DCIT:

- Je držitelem certifikátu NBÚ pro přístup k utajovaným informacím: https://www.dcit.cz/download/DCIT-NBU-osvedceni.pdf
- Je držitelem certifikátu managementu kvality dle normy ČSN ISO 9001: https://www.dcit.cz/download/DCIT-ISO9001-cs.pdf
- Má sjednáno pojištění odpovědnosti za škodu pro služby, které jsou předmětem jejího podnikání, s limitem plnění 20 milionů Kč. Certifikát o sjednaném pojištění: https://www.dcit.cz/download/DCIT-Pojisteni.pdf
- Výroční zprávy společnosti DCIT, a.s. jsou k dispozici na adrese: https://www.dcit.cz/cs/firma/pro-akcionare

Společnost DCIT disponuje týmem kvalitních odborníků, kteří jsou:

- Členové odborných sdružení a asociací (např. ISACA – Information Systems Audit and Control Association).
- Držitelé odborných certifikátů (např. CISA – Certified Information Systems Auditor, CRISC – Certified in Risk and Information Systems Control, CEH – Certified Ethical Hacker, OSCP – Offensive Security Certified Professional).
- Prověřeni Národním bezpečnostním úřadem pro stupeň Důvěrné.
- Držiteli certifikace EU GDPR DPO („Certified EU General Data Protection Regulation Data Protection Officer“, Pověřenec pro ochranu osobních údajů).

Uvedené certifikáty a prověření jsme připraveni patřičně doložit.