Smlouva č. OBE/22/02/255

Objednatel:	**Dodavatel:**
Nemocnice Třebíč, příspěvková organizace	Axians redtoo s.r.o.
Jejkov, Purkyňovo nám. 133/2	Krč, Na strži 2097/63
674 01 Třebíč	14000 Praha
IČO: 00839396	IČO: 24236594
DIČ:CZ00839396	DIČ: CZ24236594

Datum vystavení objednávky:

Datum dodání:

Místo dodání: Nemocnice Třebíč, příspěvková organizace

Způsob dodání:

Předmět:

Penetrační testy

Interní penetrační testy.
Testování interní IT infrastruktury a její bezpečnosti. Výstupem testování bude zpráva, která bude obsahovat veškeré identifikované zranitelnosti a vektory útoků, včetně analýzy dopadů a doporučení na opravu.
Cenová nabídka č. 3562, verze 1.0 tvoří nedílnou součást smlouvy

Cena celkem bez DPH:	140 000,00
DPH:	29 400,00
Cena s DPH:	169 400,00

Částky jsou uvedeny v Kč

Záruční podmínky

Práce:

Materiál:

Dodavatel výslovně souhlasí se zveřejněním celého textu této smlouvy v informačním systému veřejné správy – Registru smluv.
Smluvní strany se dohodly, že zákonnou povinnost dle § 5 odst. 2 zákona o registru smluv splní objednatel.

Vyřizuje:

Tel.:

Mobil:

E-mail:

Dne: 7. 3. 2022

Ing. Eva Tomášová
Ředitel

Dne: 7. 3. 2022

Dodavatel
Shane Crawford-Lann
Ing. Jiří Polák

Penetračního testování

Interní penetrační test

Nemocnice Třebíč, příspěvková organizace
Nabídka 3562, Version 1.0

Penetračního testování
Nemocnice Třebíč, příspěvková organizace

Nabídka
Version 1.0

Příjemce nabídky
Nemocnice Třebíč, příspěvková organizace
Purkyňovo nám. 133
674 01 Třebíč
Czech Republic

Kontaktní osoba (Objednavatel):

[redacted]
Nemocnice Třebíč, příspěvková organizace
Purkyňovo nám. 133
674 01 Třebíč
Czech Republic

Kontaktní osoba (Dodavatel):

[redacted]

Axians redtoo s.r.o
Holandská 859/3
639 00 Brno
Czech republic

[redacted]

TABLE OF CONTENTS

1 PŘEDSTAVENÍ AXIANS GROUP

1.1 O nás – Axians redtoo s.r.o.

Česká společnost **Axians redtoo s.r.o.**, založena v roce 2012, patří do nadnárodní skupiny VINCI Energies, brandu Axians. Axians působí na trhu již více než 30 let, v 22 zemích a má přes 10 000 zaměstnanců.

V České republice je společnost dlouhodobým partnerem nadnárodních i národních firem. Poskytuje unikátní portfolio služeb a řešení, do kterého patří: **kybernetická bezpečnost**, **cloudové služby** a služby **datových center**, **podnikové sítě**, **DMS** a **pracovní postupy** (workflow), **podnikové aplikace** a **analýza dat**, **systémové integrace** a **IT podpora**.

Axians se u zákazníků zaměřuje na podporu digitální transformace a nových výzev – od plánování a návrhu změn přes implementaci až po následný provoz. Klientům flexibilně a bezpečně přizpůsobuje své podnikové procesy a systémy, ochranu jejich konkurenceschopnosti, rozvíjení nového tržního potenciálu a zároveň jim optimalizuje finanční náklady na rozvoj a provoz.

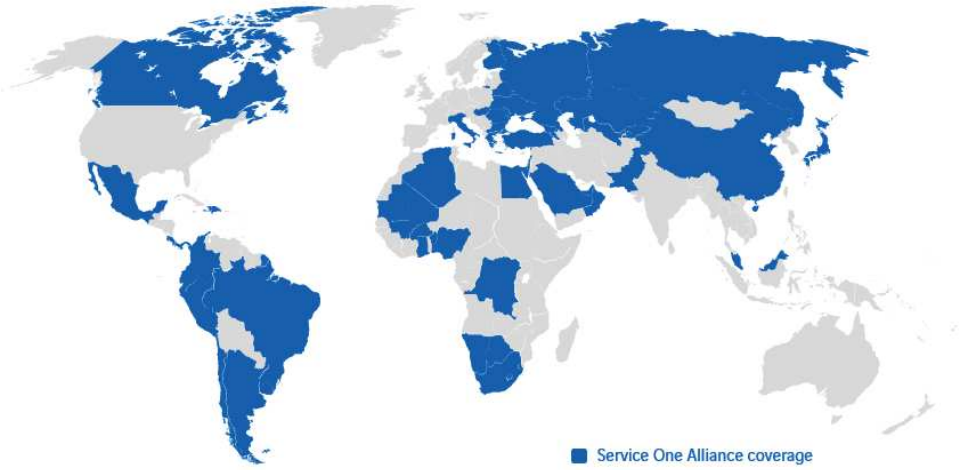
Axians redtoo je flexibilní a agilní společnost, která neustále roste a rozvíjí svou nabídku služeb. Díky proaktivní spolupráci týmů napříč divizemi, s podporou silné mezinárodní skupiny Axians a kooperaci s tisíci Axians odborníky po celém světě, dokáže nabídnout to nejlepší řešení pro své klienty.

Portfolio společnosti pokrývá následující oblasti a dodavatelské služby:

- ✓ **Infrastrukturní služby** (IMAC služby, včetně ekologické likvidace)
- ✓ **IT podpora** (v místě, vzdáleně, podpora koncových uživatelů)
- ✓ **Bezpečnostní služby** (Správa zranitelností, dodržování zásad – policy compliace, průnikové testy, SIEM, bezpečnostní monitoring, správa identit, PKI, ochrana dat proti odcizení)
- ✓ **Cloudové služby** (Microsoft Azure, Office 365, IaaS, PaaS, SaaS)
- ✓ **Správa pracovních stanic** (OS & SW Vývoj, balíčkování (App-V, MSI), EMS, SCCM)
- ✓ **Projektové řízení** (jako služba nebo práce na kontrakt)
- ✓ **Průmyslové IT** (IT-OT prostředí, Funkční testy-FAT, Síťová segmentace)
- ✓ **Služby dodávek IT** (Nákup Hardware a Software a jejich správa)
- ✓ **Podnikové aplikace a kolaborační nástroje** (správa dokumentů, řízené pracovní postupy, inranety, teamové a projektové řešení)
- ✓ **Dolování dat a jejich reportování (**ETL, dashboards, BI)
- ✓ **IT konzultace a poradenství** (kontrola způsobilosti IT, strategie, plány a návrhy řešení, audity)

1.2 Service One-Alliance – Celosvětové pokrytí

Axians je členem Service One Alliance která umožnuje poskytovat služby ve více než **80 zemích celosvětově**, je-li to za potřebí.



1.3 Významní partneři

2 PŘEDMĚT PLNĚNÍ

Na základě předešlé komunikace Axians níže předkládá návrh na provedení ***interních penetračních testů***.

Termín testu bude dohodnut po schválení objednávky.

Výstupem testování bude závěrečná zpráva, která bude obsahovat veškeré identifikované zranitelnosti a vektory útoku, včetně analýzu dopadů a doporučení na opravu. Závěrečná zpráva je blíže specifikovaná v následující kapitole.

2.1 Interní penetrační test

Bude zahrnovat celou interní IT infrastrukturu společnosti.

Před samotným zahájením budou definovány systémy, které se budou z testu vyjmuty z důvodu kritičnosti.

Interní penetrační test bude neautentizovaný (přístup k síťové zásuvce) a autentizovaný (přístup k oprávněním běžného uživatele).

Interní penetrační test bude realizován v jedné lokalitě, a to **Purkyňovo nám. 133, 674 01 Třebíč**. Interní penetrační test se mimo jiné zaměří na otestování:

3 PROVEDENÍ PENETRAČNÍHO TESTU A VÝSTUPY

Metodika penetračních testů dodavatele vychází ze standardů ***The Open Source Security Testing Methodology Manual*** (OSSTMM) a ***Penetration Testing Execution Standard*** (PTES) pro externí i interní penetrační testy.

Pro testování webových aplikací bude použit především standard ***The Open Web Application Security Project*** (OWASP) – Web Security Testing Guide v4.1.

Využití těchto standardů v kombinaci s interní metodikou a postupy dodavatele zajišťují vysokou kvalitu a konzistentní výsledky prováděných penetračních testů. Jednotlivé postupy jsou kontinuálně aktualizovány na základě dostupnosti nových zranitelností hardwaru a softwaru a na základě dostupnosti nových testovacích nástrojů a postupů.

3.1 Externí penetrační test

Externí penetrační testy jsou používány na posouzení zabezpečení společnosti a její sítě. Tento typ testu běžně zahrnuje prvky jako jsou servery, síťové zařízení, specializovaná zařízení, aplikační služby a další.

Průzkum: V této fázi jsou shromažďovány informace, které by mohly být zneužity pro pokus o napadení sítě externím útočníkem. Je kladen velký důraz na odhalení potenciálních problémů díky důslednému zkoumání všech informací zjištěných během tohoto průzkumu. Cílem průzkumu je především porozumění celkové architektuře a provozu systémů, služeb a aplikací zákazníka.

Výstupem této fáze je seznam aktivních systémů, otevřených portů, aplikací a služeb s jejich verzemi. Mezi základní nástroje v rámci této fáze testu patří *whois, nmap, bezpečnostní scanner Qualys, dnsmap, Dnsrecon, Shodan* a další. Nástroje se mohou lišit na základě konkrétních služeb a systémů. Mezi další zdroje informací patří zveřejněné seznamy uniklých e-mailových adres a hesel, které můžou být dostupné na službě pastebin, případně na internetových fórech určená k publikaci podobných informací.

Analýza zranitelností a modelování hrozeb: V další fázi je test zaměřen na odhalování zranitelností v systémech a aplikacích které mohou být zneužity útočníkem. Jako základní vstup slouží výsledky z předchozí fáze. Podle zjištěných verzí systémů a služeb dochází k identifikaci zranitelností z veřejně dostupných zdrojů.

Dále dochází k aktivnímu vyhledávání dalších zranitelností způsobených nevhodným nasazením systému nebo jeho nevhodnou konfigurací.

Dále v této fázi dochází k analýze fungování infrastruktury jako celku i jednotlivých systémů a k definici základních typů hrozeb pro cílovou síť a také rizik, která s sebou tyto hrozby nesou a jakým způsobem mohou ovlivnit další systémy. Mezi nejčastější rizika patří únik informací nebo nedostupnost systémů a služeb. Mezi hlavní nástroje v této fázi patří *OWASP Threat Dragon, Microsoft Threat Modeling Tool, PyTM* a další. Pro kategorizaci zranitelností pak může být využita některá z vhodných metodologií jako jsou CVSS nebo OWASP.

Zneužití (exploitace) zranitelností: V této fázi dochází k pokusu o zneužití objevených zranitelností a chyb (nasazení, konfigurace). Cílem je získání přístupu do systému nebo aplikace a získání citlivých dat. Mezi hlavní nástroje použité v této fázi patří: *Aircrack-ng, THC Hydra, John the Ripper, Metasploit Framework, netcat, Burp Suite Scanner, OWASP ZAP, BeEF, sqlmap* a desítky dalších. Pro zjednodušení a testování můžou být také použity vlastní skripty a pomocné programy. Použití nástrojů je zvoleno individuálně na základě dostupných aplikací a služeb, které se nachází na cílovém systému.

Post-exploitace: Hlavním cílem posledního kroku penetračního testu je eskalace práv z uživatele na administrátora (lokálního, doménového) a získání přístupu k dalším systémům. Součástí této fáze je pochopení role systému, komunikace s ostatními systémy, obsah diskového prostoru, běžící procesy, existující skripty, výčet existujícího softwaru, uživatelské a aplikační účty, lámání jejich hesel, získání přístupu do databáze, analýza operační paměti serveru apod. V této fázi jsou použity podobné nástroje jako v exploitační fázi. Tyto nástroje mohou být doplněny o další vhodné nástroje či jinak upraveny, aby umožnily další exploitaci systémů.

3.2 Interní penetrační test

Interní penetrační testy jsou používány na posouzení zabezpečení společnosti a její sítě z pohledu útočníka, který byl již schopen prolomit zabezpečení perimetru a má přístup do vnitřní sítě organizace.

Cílem interního penetračního testování může také být ověření stavu bezpečnosti a účinnost interních opatření proti možnosti eskalace oprávnění běžného uživatele na takovou úroveň, která by umožnila přístup k datům, ke kterým nemá přiděleno oprávnění.

Interní penetrační test má obdobnou strukturu jako externí penetrační test, tedy **Průzkum**, **Analýza**, **Exploitace**, **Post-Exploitace** s následujícím doplněním:

- Ve fázi **Průzkum** dochází k využití rozdílných nástrojů a přístupů, jedná se například o enumeraci *DHCP, DNS, ARP, NETBIOS, LDAP* a dalších interních služeb.

  Mezi typické nástroje potom patří: nmap, nslookup, Wireshark, arp-scan, dnsrecon, snmpwalk, tcpdump a další.

V rámci interního penetračního testu dojde k otestování infrastruktury zákazníka jak z pohledu anonymního útočníka (s přístupem k síti), tak z pohledu autentizovaného uživatele s běžným uživatelským účtem (a přístupem do uživatelského segmentu sítě).

3.3 Testy bezdrátových sítí

Penetrační testy bezdrátové sítě mají za cíl odhalit zranitelnosti, nevhodnou konfiguraci a také vhodnost využitých kryptografických algoritmů. Během testu dojde nejprve k získání údajů o bezdrátových přístupových bodech, použitých algoritmech a způsobu autentizace a šifrování za využití pasivního odposlouchávání.

Samotný penetrační test bude mít dvě fáze. V první fázi bude test probíhat z pohledu neautorizovaného útočníka a dojde k pokusu o získání neautorizovaného přístupu následujícími způsoby:

- **Slovníkový útok** vůči autentizační metodě s využitím slovníku vytvořeného na míru pro zadavatele v rozsahu minimálně 1000 hesel.
- **Odposlech autentizačních údajů** od legitimních uživatelů přímo z jejich komunikace s legitimním přístupovým bodem,
- **Analýza dostupných databází** s hesly, která byla publikována v prostředí Internet / Darknet s vazbou na pracovníky objednatele.

Testování Captative portálu (pokud existuje)

Druhá fáze testu probíhá z pohledu autentizovaného uživatele do návštěvnické sítě. Penetrační test se zaměří na oddělení této části sítě od zbytku infrastruktury. Samotný průběh testu je obdobný jako u externího penetračního testu.

Pro penetrační test bezdrátové sítě budou použity především následující nástroje: Aircrack-ng, CloudCracker, AirSnort, Cain & Abel, Airjack a další.

4 ZÁVĚREČNÁ ZPRÁVA

Na závěr jsou jednotlivé testy vyhodnoceny a je vypracována závěrečná zpráva. Během celého testu dochází k detailnímu zaznamenávání všech akcí provedených během penetračních testů s přesným časovým údajem. Pokud dojde k jakékoli změně na testovaných systémech nebo aplikacích, jsou tyto změny komunikovány s vlastníky těchto systémů / aplikací a budou také součástí závěrečné zprávy. Struktura závěrečné zprávy bude následující:

- **Manažerský souhrn**: shrnutí průběhu testů a nejzávažnějších nálezů, doporučení k nápravě
- **Popis metodiky** a klasifikace zranitelností
- **Popis testu:** použitá metodika, přehled všech činností, použité nástroje a časový harmonogram průběhu testu
- **Zjištěné skutečnosti:** detailní popis výsledku všech testů jednotlivých zařízení, zjištěné zranitelnosti, příklad možného útoku a důsledky plynoucí ze zneužití dané zranitelnosti
- **Doporučení**: seznam doporučení, kterými lze odstranit nedostatky a zranitelnosti nalezené během testování
- **Závěr**

5 NABÍDKOVÁ CENA

V souladu s poptávkou zadavatele nabízí předkladatel cenovou nabídku:

Položka	Cena v Kč bez DPH
Interní penetrační test	140 000,-
Celkem bez DPH	**140 000,-**
Celkem s DPH	**169 400,-**

Ceny uváděny v Kč a zahrnují cestovní náklady.

5.1 Garance ceny

Předkladatel garantuje, že uvedené ceny jsou maximální, nepřekročitelné a zahrnují veškeré náklady předkladatele na plnění dle této nabídky. V případě, že v průběhu realizace zakázky bude zjištěno, žerozsah prací bude nižší o více než 15% z předpokládaného a nabízeného plnění, Dodavatel garantuje,že bude neprodleně informovat Objednatele a adekvátně po dohodě s Dodavatelem odpovídajícím způsobem sníží rozsah plnění a cenu za poskytnuté plnění.

5.2 Obchodní a platební podmínky

Daňový doklad/fakturu vystaví Dodavatel neprodleně po podpisu předávacího a akceptačního protokolu.

DPH bude fakturována dle účinných právních předpisů v době fakturace.

Lhůta splatnosti daňového dokladu-faktury je čtrnáct dní (14) den ode dne jejich doručení Objednateli. Daňový doklad-faktura se považuje za doručenou tři dny po jejím prokazatelnémodeslání. Faktura bude uhrazena bankovním převodem na účet druhé smluvní strany.

Nebude-li daňový doklad-faktura obsahovat náležitosti stanovené § 28, odst. 2 zák. č. 235/2004 Sb., odani z přidané hodnoty, ve znění pozdějších předpisů, nebo v ní nebudou správně uvedené údaje, je Objednatel oprávněn vrátit ji ve lhůtě splatnosti Poskytovateli s poukázáním na chybějící náležitosti nebo nesprávné údaje. V takovém případě se přeruší doba splatnosti a nová lhůta splatnosti počne běžet doručením opravené faktury Objednateli.

6 PROHLÁŠENÍ PŘEDKLADATELE

Předkladatel prohlašuje, že je vázán celou svou nabídkou do 28.02.2022.