VŠEOBECNÁ FAKULTNÍ NEMOCNICE V PRAZE
U Nemocnice 499/2, 128 08 Praha 2 | IČ: 00064165, DIČ: CZ00064165

OBJEDNÁVKA č. 70 037/26

Vyřizuje/Telefon:	P. Kostrhová/ +420 224 969 292	**Prodávající:**	ATS-TELCOM PRAHA a.s. Nad elektrárnou 1526/45 106 00 Praha 10
Termín plnění:	1.3. - 31.3.2026		
Místo plnění:	VFN, U Nemocnice 2, Praha 2	**IČ:**	**61860409** **DIČ: CZ61860409**
		Kontakt:	
Osoba oprávněná k převzetí předmětu plnění: p.Roman Skuhra tel.: 22496 9378, e-mail: roman.skuhra@vfn.cz		**Tel./e-mail:**	jindrich.kolar@atstelcom.cz

Číslo pol.	Předmět plnění	Cena za MJ (MD)bez DPH	Sazba DPH	Cena za MJ s DPH	Množství (ČH)	Cena za položku včetně DPH
1	Provedení penetračních testů aplikace SHACL (sklad a aplikace centrových léků)	990,00 Kč	21%	1 197,90 Kč	64	76 665,60 Kč
	viz příloha č. 1 této objednávky, dle smlouvy PO 944/S/25, max. 8MD					

Fakturační adresa Všeobecná fakultní nemocnice v Praze Ekonomický úsek - Odbor účetnictví U Nemocnice 499/2, 128 08 Praha 2	**Cena celkem bez DPH**	**63 360,00 Kč**
	Cena celkem s DPH	**76 665,60 Kč**

Platba po dodání. Na fakturu a dodací list/akceptační protokol uveďte číslo této objednávky. PP je možno dodat ihned po oboustranném podepsání objednávky. Celková cena uvedená v objednávce je konečná a nejvýše přípustná pro PP dle specifikace v objednávce. Celkovou cenu lze překročit pouze při prokazatelé změně DPH, a to pouze ve výši shodné s tímto navýšením. Celková cena zahrnuje veškeré náklady spojené s realizací PP. Prodávající je povinen, po vzniku práva fakturovat, vystavit a objednateli předat fakturu ve dvojím vyhotovení s rozepsáním položek PP přesně dle objednávky a uvedením jejich jednotkových cen. K faktuře bude přiložena kopie řádně opatřeného dodacího listu/akceptačního protokolu potvrzeného osobou oprávněnou k převzetí/akceptaci PP s uvedením záruční doby PP a v případě relevantvosti s uvedením všech výrobních, sériových a produktových čísel – bez tohoto dokladu nelze fakturu proplatit. Vystavená faktura musí obsahovat všechny náležitosti řádného daňového dokladu dle platné právní úpravy. V případě, že faktura nebude obsahovat všechny požadované náležitosti, je oprávněn ji objednatel do 15 dnů prodávajícímu vrátit k opravě a doplnění. Dnem nového doručení faktury začíná běžet nová lhůta splatnosti faktury. Splatnost faktury se sjednává na 60 dní ode dne jejího doručení objednateli. V případě prodlení objednatele s úhradou řádně fakturované ceny je prodávající oprávněn požadovat zaplacení smluvního úroku z prodlení ve výši 0,01 % z nezaplacené částky za každý i započatý den prodlení. Prodávající je oprávněn požadovat zaplacení úroku z prodlení až po uplynutí 30 dn ů od sjednané lhůty splatnosti. Objednatel je oprávněn požadovat zaplacení smluvní pokuty ve výši 0,1% z celkové kupní ceny bez DPH za každý i započatý den prodlení s dodáním zboží. Faktura bude zaslána elektronicky ve formátu PDF na adresu faktury@vfn.cz. Akceptační protokol bude přiložen v nascanované podobě. Prodávající bere na vědomí, že dodávané technické nebo programové prostředky nesmí být prostředky, které jsou zveřejněny na stránkách Národního centra kybernetické bezpečnosti (provozované NÚKIB, https://nukib.gov.cz/) za hrozbu, k datu uzavření objednávky/smlouvy. Veškeré poskytované služby, po dobu platnosti smlouvy nebo po dobu časového vymezení objednávky, nesmí být provozované na výše uvedených technických nebo programových prostředcích označených NÚKIB za hrozbu. Prodávající bere na vědomí, že objednatel je povinen dle zákona č. 340/2015 Sb. o registru smluv, ve znění pozdějších předpisů, uveřejnit tuto objednávku včetně případných dodatků zákonem stanoveným způsobem.

Počet listů: -1-	**Přílohy: 1/3**	Poznámka: NS 15000

Objednávku přijímám a souhlasím s podmínkami

Datum:	Datum: 10.2.2026
Prodávající:	Objednatel: Ing. Michal Jelínek Náměstek ředitele pro Informatiku a digitální transformaci
Razítko:	

Penetrační test aplikace „Skladové hospodářství a podávání centrových léků“ (SHACL)

Specifikace objednávky

Rozsah testu

1. Předmětem služby bude jednorázový penetrační test aplikace skladového hospodářství a zaznamenávání podávání centrových léků na externích aplikačních centrech (SHACL) prostřednictvím testování aplikační vrstvy přímo u výrobce/dodavatele SW v jeho testovacím prostředí v kombinaci s testy externího přístupu a testů infrastruktury komponent aplikace v produkčním prostředí dle přílohy č. 4 smlouvy PO 234/S/25, přístupného na dodaných IP adresách/DNS záznamech (viz IP adresy/DNS záznamy).
2. Pro poskytnutí služby je využito automatizované nástroje a skripty pro automatizované testování zranitelností. Objednatel požaduje ověření minimálně 2 nástroji (např. Metasploit, Nessus Vulnerability Scanner, Shadow Security Scanner, Nmap, SuperScan, Burp Suite, Owasp ZAP, SQLmap, Kali Linux, Jawfishp apod.), aby byla zajištěna komplexnost testování zranitelností. Nástroje mohou být různě kombinovány dle typu testu a způsobu ověření. Poskytovatel musí do výstupu uvést, jaké nástroje a pro jaký typ testování použil. Seznam identifikovaných zranitelností bude součástí výstupu včetně detailního popisu zranitelnosti, její závažnosti a doporučení pro její odstranění či eliminaci hrozby s ní spojené. Při nálezu zranitelnosti zpravidla dochází k jejímu zaznamenání, nikoliv k dalšímu průniku do informačního systému, který je předmětem skenování, jako by tomu bylo u penetračního testování.
3. V případě zjištění zranitelnosti, která umožňuje hlubší průnik do systému objednatele, poskytovatel musí provést manuální testování s využitím uvedené zranitelnosti s cílem dosáhnout částečného nebo úplného převzetí systému, případně oprávnění, která mu nenáleží. Hlavní důvod manuálního ověření nebo jiné verifikace u nálezů je vyřazení „False positive“ nálezů a prověření případů, u kterých dle expertního odhadu existuje vysoké riziko zneužití útočníkem. Součástí závěrečné zprávy musí být zjištění získaná v průběhu testování včetně negativních zjištění (zranitelnost nebylo možné využít). Manuální ověření nebo jiná verifikace musí být provedena u všech zjištěných zranitelností skenováním nebo automatizovanými testy označené za kritické a vysoké zranitelnosti nebo opakující se u více systémů/služeb se střední zranitelností obdobného typu. V případě pozitivních zjištění poskytovatel podrobně popíše dosažený výsledek a současně i okolnosti, které mu tento výsledek umožnily dosáhnout (slabá hesla, nesprávné verze protokolu atd.).
4. Poskytovatel provede testování určených aplikací objednatele, uvedených výše, a to způsobem, který je v souladu s metodikami (např. OWASP WSTG v. 4.2, OWASP ASVS v. 5, PTES, OSVDB, OSSTMM, TIBER-EU). Minimální rozsah testů musí pokrývat OWASP Top 10 v aktuální podobě nebo jiné nejčastěji zjištěné zranitelnosti.

5. Testy budou realizovány s přihlášením, bez znalosti architektury nebo infrastruktury aplikace, které budou zaměřené na zranitelnosti této aplikace v prostředí dodavatele řešení. Aplikace je umístěna za loginem, který bude dodavateli sdělen.
6. Součástí závěrečné zprávy budou zjištění získaná v průběhu testování. V případě pozitivních zjištění poskytovatel podrobně popíše dosažený výsledek a současně i okolnosti, které mu tento výsledek umožnily dosáhnout (nedodržení doporučených postupů, nesprávné verze knihoven atd.).
7. Předmětem testu budou aplikace/systémy a infrastruktura, dostupné pod IP adresními rozsahy používanými Objednatelem.

IP adresy/DNS záznamy

IP adresy/DNS záznamy VFN k datu objednávky:

Používané adresy	**DNS; použití**
91.99.232.92	https://shacl.medoro.one/

Součástí objednaných služeb bude:

1. Každá identifikovaná zranitelnost ručně validovaná musí mít ve výstupech uvedeno minimálně následující:
    - detailní seznam zjištění, minimálně v rozsahu:
    - identifikace zjištění zranitelnosti,
    - popis kde a jakým způsobem byla zranitelnost identifikována,
    - označení/název zranitelnosti (pokud lze přiřadit),
    - charakteristika zranitelnosti včetně potenciálního dopadu,
    - klasifikace zranitelnosti podle použité metodiky, kde bude obsaženo:
        - kategorii/typ zranitelnosti,
        - úroveň zranitelnosti,
        - dle pravděpodobnosti zneužití,
        - náročnosti odstranění/nápravy.
    - popis zranitelného místa/nálezu,
    - navržené opatření nebo doporučení k eliminaci nebo minimalizaci zranitelnosti, případně odkazy na doporučení výrobce/distributora nebo jiné best practice,
    - další využití zranitelnosti, pokud bylo v rámci manuálních testů,
    - další podstatné skutečnosti,
2. Součástí výstupu bude i excelovský soubor, který bude obsahovat celkový přehled identifikovaných zranitelností (včetně nízkých zranitelností) a ručně validované minimálně ve struktuře uvedené v bodě 1., kdy každá zranitelnost bude na jednom řádku.

3. Nastavení automatizovaného nástroje bude uloženo nebo zdokumentováno u poskytovatele, aby byla zajištěna opakovanost testu v případě ověření odstranění zranitelností, a bylo možné odlišit nově zařazené nebo jinak hodnocené zranitelnosti. Doba uložení je 3 měsíců od realizace testu nebo do sdělení o jejich smazání Objednatelem.

Omezení nebo požadavky na dodání služby

1. Automatizovaný test bude probíhat pouze v definovaný den a časovém rozmezí stanovený Objednatelem po odsouhlasení dodavatele služby. Předpokladem je, že testy budou probíhat mimo hlavní vytížení provozu nemocnice (pokud nebude domluveno jinak), např. v pátek po 18 hod.
2. Ruční ověření bude probíhat v dohodnutém čase a jeho směřování bude stanoveno na základě pravděpodobnosti ohrožení nebo omezení provozu nebo fungování ICT VFN.
3. Veškeré testy či manuální ověření budou prováděny bez destruktivních zásahů tzn., že útok končí identifikací zranitelnosti, neprovádějí se žádné změny nebo požadavky nad rámec těch, které jsou automatizovaným nástrojem běžně v rámci testů zasílány, které by poškodily, znepřístupnily či jinak ohrozily provoz/fungování informačních systémů nebo infrastruktury VFN.
4. V případě zjištění nebo upozornění Objednatelem při provádění testu či manuálním ověření na možné nebo probíhající poškození, znepřístupnění či jiné ohrožení provozu či fungování informačních systémů nebo infrastruktury VFN, je Objednatel povinen neprodleně učinit takové kroky a opatření, které zamezí pokračování nebo ukončí všech činností, které způsobily nebo signalizují tyto negativní dopady.
5. Body 2 až 4 se nevztahují na testování v testovacím prostředí dle specifikací (IP rozsah apod.) objednatele či dodavatele aplikace/systému, ale za předpokladu, že testy neovlivní jiné než testovací prostředí (např. vývojové, produkční, zálohovací).
6. Tety či manuální ověření musí být prováděny tak, aby nehrozily nebo nezpůsobily škody třetí osobě. Vyjma třetích osob, které patří mezi provozovatele/poskytovatele nebo dodavatele ICT a jsou s infrastrukturou VFN propojeni. U této výjimky je nutné dodržet zásady uvedené v bodě 3. a 4.
7. V případě zjištění nebo podezření na souběžně probíhající skenování, testy nebo kybernetický útok, musí být provedeny nezbytné kroky k zdokumentování a zajištění forenzních důkazů a okamžitému nahlášení kontaktní osobě za VFN (viz kontaktní osoby), která rozhodne, zda budou testy ukončeny nebo pokračováno, a za jakých podmínek.

Kontaktní osoby

- **Za průběh testů:**

- **Za objednávku a akceptaci:**