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

OBJEDNÁVKA č. 70 238/21

Vyřizuje/Telefon: P. Kostrhová/ +420 224 969 292
Termín plnění: do 31.8.2021
Záruční doba:
Místo plnění: VFN, U Nemocnice 2, 128 08, Praha 2

Osoba oprávněná k převzetí předmětu plnění (PP):
Ing. Michal Jelínek
Tel: +420 22496 9517 e-mail: michal.jelinek@vfn.cz

Dodavatel: ESET software spol. s r.o.
Jankovcova 1037/49
170 00 Praha 7
IČ: **26467593** **DIČ:** **CZ26467593**
Kontakt: p. Jaroslav Lom
Tel./e-mail: 420 603 555 526 lom@eset.cz

Z důvodu připravenosti k převzetí PP žádáme o tlf. vyzvání před dodáním v pracovní době, tj. v pondělí-pátek 7:00-15:30.

Číslo položky	Předmět plnění	Cena za MJ bez DPH	Sazba DPH	Cena za MJ s DPH	Množství	Cena za položku včetně DPH
	Ověření zranitelností - Portál pacienta					
1	Ověření zranitelností dle rozsahu aplikace	26 400,00 Kč	21%	31 944,00 Kč	1	31 944,00 Kč
2	Assessment Azure Resources	26 400,00 Kč	21%	31 944,00 Kč	1	31 944,00 Kč
	Termín realizace do 31.8.2021, pokud nebude dohodnuto mezi Objednavatelem a dodavatelem jinak. Dle cenové nabídky uvedené v příloze					

Fakturační adresa
Všeobecná fakultní nemocnice v Praze
Ekonomický úsek - Odbor účetnictví
U Nemocnice 499/2, 128 08 Praha 2

Cena celkem bez DPH	**52 800,00 Kč**
Cena celkem s DPH	**63 888,00 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 – 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 dnů 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 může být zaslána i elektronicky ve formátu PDF nebo ISDOC na adresu faktury@vfn.cz. V případě, že bude faktura zaslána elektronicky, bude dodací list přiložen v nascanované podobě. Dodavatel bere na vědomí, že dodávané technické nebo programové prostředky nesmí být prostředky, které jsou zveřejněny na stránkách Národního centra kybernetické bezpečnosti (provozované NÚKIB, https://www.govcert.cz/) a označeny jako varování nebo hrozba v době uzavření objednávky. Veškeré poskytované služby nesmí být provozované na výše uvedených technických nebo programových prostředcích označených NÚKIB jako varování nebo hrozba.

Počet listů: -1-	**Přílohy: 1/5**	Poznámka: NS 15060

Objednávku přijímám a souhlasím s podmínkami

Datum:	Datum: 30.6.2021
Prodávající:	Objednatel: Ing. Ivan Veselý, MBA Náměstek ředitele pro Informatiku a digitální transformaci
Razítko:	*Razítko:*

Ověření zranitelností – Portál pacienta

Specifikace objednávky

Rozsah ověření zranitelností

1. Předmětem služby bude jednorázové ověření zranitelností v Portálu pacienta v části e-Recepty, přístupných na webové stránce *test-pacient.vfn.cz*. Předmětem ověření je zhodnocení bezpečnostního stavu aplikace Portál pacienta, části e-recepty. Ověření aplikační logiky proběhne na testovacím prostředí, assessment konfigurace azure prostředků proběhne na produkčním prostředí. Cílem ověření bude prověření bezpečnosti aplikace podle metodiky OWASP Testing Guide.
2. Ověření bude provedeno pouze v předem definovaném časovém okně, které bude dostatečně dopředu fixováno.
3. Hlavním cílem ověření bude prověřit možnost získání přístupu k cizím datům a hledat výskyt různých technických zranitelností publikovaných v OWASP Testing Guide a jiných zdrojích. Prováděné ověření budou realizovány „semi-automaticky“, kdy v relevantních částech jsou prováděny ověření s využitím automatizovaných nástrojů. Výstupy z automatizovaných nástrojů jsou následně manuálně verifikovány konzultanty s cílem očistit výsledky automatizovaných ověření o „false-positive“ nálezy tj. nalezené zranitelnosti ve skutečnosti neexistují. Vedle automatizovaných ověření jsou prováděny manuální ověření v těch částech, kde v současné době dostupné nástroje nelze v plné míře nebo zcela použít.
4. Ověření bude provedeno v režimu „grey box“, kdy konzultanti během ověření budou spolupracovat se zadavatelem a budou vycházet z jím poskytnutých informací.
5. Výběr prověřovaných zranitelností bude vycházet především ze zkušeností testerů s podobnými projekty.
6. Ověření a použitých metodikách jsou uvedeny v kapitole Použité metodiky a nástroje.

Použité metodiky a nástroje

Obecné zásady

Při ověření musí být dodrženy tyto principy:

- Ověření musí být vždy koncipována s ohledem na byznys potřeby VFN.
- Ověření musí být metodické a opakovatelné.
- Včasné upozorňování na možná rizika související s prováděným ověřením.
- Výsledky ověření jsou interpretovány s ohledem na celkový dopad a závažnost zjištění.

Metodika OSSTMM

Jako základ pro bezpečnostní ověření musí být využit mezinárodní standard OSSTMM – Open Source Security Testing Methodology Manual.

Metodika OWASP

Pro ověření webových aplikací a služeb se musí vycházet z metodik, které jsou vytvářeny v rámci projektu OWASP (The Open Web Application Security Project - www.owasp.org) s využitím klíčové metodiky/příručky „OWASP Testing Guide“ ve revizi 4.2 nebo vyšší, doplněné o vybrané kapitoly z připravované verze 5. Ověření webových aplikací rozdělených do následujících oblastí:

- Information Gathering
- Configuration and Deployment Management
- Identity Management Testing
- Authentication Testing
- Authorization Testing
- Session Management Testing
- Input Validation Testing
- Testing for Error Handling
- Testing for weak Cryptography
- Business Logic Testing
- Client Side Testing

Pro prezentaci výsledků ověření webových aplikací a služeb, které budou provedeny v souladu s metodikou OWASP Testing Guide, bude použita metodika OWASP TOP 10, aby bylo docíleno co nejlepšího přehledu výsledků. Výčet nejkritičtějších oblastí zranitelností uvedených v OWASP TOP 10 je také využit pro omezení rozsahu prováděných ověření u webových aplikací, kde není nezbytné provádět ověření plně v souladu metodikou OWASP Testing Guide.

Způsob prováděného ověření zranitelností

Ověření musí představovat nejpřesnější simulaci reálných útoků, protože využívají stejné postupy jako v případě reálného útočníka. V jejich průběhu musí být kombinovány jednotlivé informace mezi sebou, aby postihly mnohem větší hloubku, než např. samotné skenování známých zranitelností.

V první části bude snahou identifikovat a využít nejpravděpodobnějších a nejvíce viditelných či snadných slabin systému. Ve druhé části bude v nutném rozsahu ověřovány i všechny ostatní možnosti útoků. Představují výzkum identifikovaných zranitelností, slabin nebo nevhodných konfigurací a jejich ověřování na ověřovaném systému.

Fáze – získávání informací

Během této fáze budou získány informace o ověřovaných systémech a VFN. Fáze je složena z několika samostatných částí, mezi které patří sbírání dat, získávání informací atd. K vyhledávaným informacím patří například:

- Informace z DNS, používané rozsahy IP adres
- Informace o poskytovatelích služeb např. ISP
- Vlastníci systémů a služeb
- Dodavatelé ICT technologií, informačních systémů atp.
- Publikované informace ze strany organizace nebo zaměstnanců
- Vazby mezi obchodními partnery atd.

Jedná se o pasivní způsob zkoumání ověřovaných systémů a VFN, kdy nedochází k žádnému nebo minimální kontaktu (nepřekračuje „běžný provoz“) s ověřovanými systémy a VFN.

Fáze – skenování

Skenování představuje aktivní způsob zkoumání ověřovaných systémů, která většinou probíhá na síťové a transportní vrstvě. Mezi získávané informace patří například:

- Otevřené, zavřené nebo filtrované síťové porty
- Informace o publikovaných službách

- Identifikace používaných operačních systémů
- Chování infrastruktury (síťové a aplikační firewally, směrování, překlad adres, IPS, anti-malware, loadbalancing atp., případně detekce a reakce na zjištěný útok)
- Identifikace zranitelných aplikací nebo služeb
- Úroveň aplikovaných bezpečnostních záplat
- Odhalování zadních vrátek (backdoor)
- Seznam možných cílů pro útoky typu DoS

V této fázi bude také proveden celkové ověření dnes známých a definovaných zranitelností pomocí vybraných automatizovaných nástrojů, které jsou zvoleny v závislosti na ověřovaných systémech.

Na základě informací získaných z této fáze bude možné určit další směr postupu ověření, který bude konzultován s kontaktní osobou Objednatele.

Fáze – pronikání

Fáze pronikání představuje finální etapu vlastního ověření. Představuje výzkum identifikovaných zranitelností, slabin nebo nevhodných konfigurací a jejich ověřování na systému. K hlavním úkolům této fáze patří:

- Ověření nalezených zranitelností a možnosti jejich zneužití proti testovaným systémům a organizaci
- Získání neoprávněného přístupu na ověřované systémy
- Získání neoprávněného přístupu k informacím nebo narušení jejich integrity
- Eskalace privilegií s cílem získání vyššího oprávnění pří přístupu na testované systémy nebo k informacím
- Realizace DoS útoku proti ověřovaným systémům

Součástí objednaných služeb bude:

1. Ruční ověření nebo jiná verifikace zjištěných zranitelností označené za vysoké a kritické zranitelnosti nebo opakující se u více systémů se střední zranitelností obdobného typu.
2. Každá identifikovaná zranitelnost ručně validovaná musí mít ve výstupech uvedeno minimálně následující:
    - Označení/Název zranitelnosti,
    - Kategorii/typ zranitelnosti,
    - Úroveň zranitelnosti,
    - Popis zranitelnosti,
    - Navržené opatření nebo doporučení k eliminaci nebo minimalizaci zranitelnosti, případně odkazy na doporučení výrobce/dodavatele nebo jiné best practice.

    Ostatní zranitelnosti budou ve struktuře výstupů z automatizovaných nástrojů.
3. Zpráva, která obsahuje popis provedení ověření, použité metodiky a postupy, souhrn zjištěných ověřených zranitelností (viz bod 1.), jejich vyhodnocení, manažerský souhrn a doporučení nebo navržené další kroky.
4. Součástí zprávy bude i excelovský soubor, který bude obsahovat celkový přehled identifikovaných zranitelností (včetně nízkých zranitelností) a ručně validované minimálně ve struktuře uvedené v bodě 2., kdy každá zranitelnost bude na jednom řádku. Excelovský soubor bude na samostatné listu obsahovat výčet nálezů ručně validovaných a vyhodnocených za „False positive“ ve struktuře výstupu z automatizovaného nástroje.

5. Nastavení automatizovaného nástroje bude uloženo nebo zdokumentováno u Dodavatele služby, aby byla zajištěna opakovanost ověření zranitelností v případě ověření odstranění zranitelností, a bylo možné odlišit nově zařazené nebo jinak hodnocené zranitelnosti. Doba uložení je 6 měsíců od realizace ověření nebo do sdělení o jejich smazání Objednatelem.

Omezení nebo požadavky na dodání služby

1. Ověření bude probíhat pouze v definovaný den a časovém rozmezí stanovený Objednatelem po odsouhlasení dodavatele služby.
2. V případě zjištění nebo upozornění Objednatelem při provádění ověření na možné nebo probíhající poškození, znepřístupnění či jiné ohrožení provozu či fungování informačních systémů nebo infrastruktury VFN, je Dodavatel povinen neprodleně učinit takové kroky a opatření, které zamezí pokračování nebo ukončí všech činností, které způsobily nebo signalizují tyto negativní dopady.
3. Ověření musí být prováděny tak, aby neohrozily 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 2.
4. V případě zjištění nebo podezření na souběžně probíhající scanování nebo kybernetický útok, musí být Dodavatelem provedeny nezbytné kroky k zdokumentování a zajištění forenzních důkazů a okamžitému nahlášení kontaktní osobě za VFN (viz kontaktní osoby), která rozhodne, zda bude ověření ukončeno nebo pokračováno, a za jakých podmínek.

Součinnost Objednatele

1. Pro potřeby koordinace činnosti a poskytovaní odpovídajících informací jsou na straně Objednatele ustanoveny kontaktní osoby (viz kap. Kontaktní osoby), které jsou odpovědné za spolupráci s Dodavatelem a která je vybavena příslušnými pravomocemi.
2. Dodavateli budou zpřístupněny informace a dokumenty, které jsou pro provedení bezpečnostních testů nezbytné. Rozsah informací a dokumentace bude odpovídat rozsahu, který mají k dispozici uživatelé aplikace, z jejichž perspektivy bude ověření prováděn, nebo jsou veřejně dostupné. Bude poskytnuta podporu v případě, že tester narazí na nesrozumitelný žargon nebo jiný problém způsobený nedostatečnou znalostí reálií z prostředí aplikace.
3. Během ověření nebude docházet ke změnám v testovacím prostředí nebo výpadkům testovacího prostředí.
4. Pro assessment azure prostředků bude zajištěn účet s právy pro čtení s přístupem do daných subskripcí (global-reader).
5. Budou dodány nezbytné URL aplikace v testovacím prostředí a konektivitu k němu.
6. Bude dodáno alespoň 10 validních kódů e-Receptů, aby bylo možné projít veškerou funkcionalitu řešení.

Kontaktní osoby

- **Za průběh testů:**
  Josef Kubr, projektový manažer
  Mob.: +420 777 997 067, Josef.Kubr@vfn.cz
- **Za objednávku a akceptaci:**
  Ing. Michal Jelínek, odbor bezpečnosti informací,
  Mob.: +420 602 650 715, michal.jelinek@vfn.cz

Cenová nabídka

Ceny testů jsou stanovena individuálně dle požadavků organizace:

- Ověření zranitelností dle rozsahu aplikace 26.400,-Kč
- Assessment Azure Resources 26.400,-Kč

Nabídková cena pro VFN: 52.800,- Kč bez DPH