Dílčí smlouva č. 2023/04825 o poskytnutí služeb

k Rámcové dohodě o poskytování služeb č. 2022/05974 ze dne 11.8.2022

Česká pošta, s.p.

se sídlem:	Politických vězňů 909/4, 225 99, Praha 1
IČO:	47114983
DIČ:	CZ47114983
zastoupen:	Mgr. Andreou Barešovou, manažerem útvaru e-GOV
zapsán v obchodním rejstříku u:	Městského soudu v Praze, oddíl A, vložka 7565
bankovní spojení:	[redacted]

dále jen „**Objednatel**“ nebo „**ČP**“

a

Ernst & Young, s.r.o.

se sídlem:	Na Florenci 2116/15, Nové Město, 110 00 Praha 1
IČO:	26705338
DIČ:	CZ26705338
zastoupena:	[redacted]
zapsána v obchodním rejstříku u:	Městského soudu v Praze, oddíl C, vložka 108716
bankovní spojení:	[redacted]

dále jen „**Dodavatel**“

dále jednotlivě jako „**Smluvní strana**“, nebo společně jako „**Smluvní strany**“

uzavírají v souladu s ustanovením § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**Občanský zákoník**“), tuto Dílčí smlouvu o poskytnutí služeb (dále jen „**Smlouva**“) k **Rámcové dohodě o poskytování služeb** ze dne 11.8.2022 (dále jen „**Rámcová dohoda**“).

Preambule

Objednatel provedl v souladu s Rámcovou dohodou soutěž o dílčí veřejnou zakázku „Penetrační testy ke kreditnímu systému“ (dále jen „**minitendr**“). Tato Smlouva je uzavřena s Dodavatelem na základě výsledku minitendru.

1. Předmět Smlouvy a podmínky plnění

1.1. Předmětem této Smlouvy je závazek Dodavatele poskytnout Objednateli řádně a včas služby zahrnující činnosti ve smyslu ust. odst. 1.2 písm. b) Rámcové dohody, konkrétně provedení penetračních testů webové aplikace před uvedením do provozního prostředí Objednatele a ověření po uvedení do produkčního prostředí.

(dále jen „**Plnění**“).

Bližší specifikace a požadavky na Plnění, které je Dodavatel Objednateli povinen poskytnout, je obsažena v příloze č. 1 této Smlouvy.

2. Cena

2.1. Maximální cena Plnění činí 120 000,- Kč (slovy: jedno sto dvacet tisíc korun českých) bez DPH. Rozklad ceny je uveden v příloze č. 1 Smlouvy. Cena za retesty bude hrazena dle skutečně provedených retestů v sazbě dle přílohy č. 1 Smlouvy, maximálně budou provedeny a uhrazeny 2 retesty.

2.2. Cena zahrnuje veškeré náklady Dodavatele spojené s plněním Dílčí smlouvy a poskytnutím plnění Objednateli. Tato cena je cenou konečnou, nejvýše přípustnou a nemůže být zvýšena bez předchozího písemného souhlasu Objednatele.

3. Práva a povinnosti Smluvních stran

3.1. Seznam osob, jejichž prostřednictvím bude Dodavatel zajišťovat plnění této Smlouvy, je uveden v Příloze č. 2 Smlouvy (dále jen „**realizační tým**“). Bude-li z důvodů vzniklých na straně Dodavatele nutné nahradit kteréhokoliv člena realizačního týmu, bude po předchozím odsouhlasení Objednatelem nahrazen novým členem týmu s odpovídající nebo vyšší kvalifikací, a to do 2 týdnů od oznámení důvodů pro nahrazení Objednateli.

4. Doba a místo plnění

4.1. Dodavatel se zavazuje poskytnout Plnění do 30 dnů ode dne nabytí účinnosti Smlouvy. Poskytování Plnění dle této Smlouvy bude zahájeno bez zbytečného odkladu po nabytí její účinnosti.

4.2. Místem poskytování Plnění je pracoviště Objednatele – Olšanská 38/9, 225 99 Praha 3.

5. Závěrečná ustanovení

5.1. Tato Smlouva nabývá platnosti dnem podpisu oběma smluvními stranami a účinnosti dnem uveřejnění Smlouvy v registru smluv. Případné plnění předmětu této Smlouvy v době od okamžiku platnosti Smlouvy do okamžiku nabytí její účinnosti se považuje za plnění podle této Smlouvy a práva a povinnosti z něj vzniklé se řídí touto Smlouvou.

5.2. Smluvní strany jsou oprávněny od Smlouvy odstoupit ze stejných důvodů a za stejných podmínek, jaké platí pro odstoupení od Rámcové dohody.

5.3. V otázkách touto Smlouvou neupravených se použijí ustanovení Rámcové dohody.

5.4. Kontaktní osoby Smluvních stran pro účely plnění této jsou následující:

Kontaktní osoba Objednatele: [redacted]

Kontaktní osoba Dodavatele: [redacted]

5.5. Tato Smlouva je vyhotovena v elektronické podobě, přičemž každá Smluvní strana obdrží její elektronický originál opatřený platnými elektronickými podpisy.

5.6. Nedílnou součástí Smlouvy jsou následující přílohy:

Příloha č. 1 – Specifikace Plnění a Cena

Příloha č. 2 – Složení realizačního týmu Dodavatele

5.7. Smluvní strany prohlašují, že tato Smlouva vyjadřuje jejich úplné a výlučné vzájemné ujednání týkající se daného předmětu této Smlouvy. Smluvní strany po přečtení této Smlouvy prohlašují, že byla uzavřena po vzájemném projednání, určitě a srozumitelně, na základě jejich pravé, vážně míněné a svobodné vůle. Na důkaz uvedených skutečností připojují podpisy svých oprávněných osob či zástupců.

V Praze	V Praze
Mgr. Andrea Barešová manažer útvaru e-GOV **Česká pošta, s.p.** *(elektronicky podepsáno)*	[redacted] **Ernst & Young, s.r.o.** *(elektronicky podepsáno)*

Příloha č. 1 – Specifikace Plnění a Cena

Penetrační test kreditních aplikací ČP

1. Předmět

Objednatel Požaduje provést penetrační testy webové aplikace před uvedením do provozního prostředí České pošty (dále jen "ČP")a ověření po uvedení do produkčního prostředí. Aplikace je kreditní povahy, a je navázána na externí platební bránu a souvisí s užíváním Informačního systému datových schránek (dále jen "ISDS") a s doplňkovými službami, které poskytuje ČP. Pojem "kredit" zde označuje předplatné služeb. Webová aplikace slouží pro dobíjení kreditu za účelem odesílání poštovních datových zpráv (dále jen "PDZ") a nastavování služby Datový trezor (dále jen „DT“). Blíže je účel a funkcionality popsán v kapitole 3.

2. Legislativa

Poskytované služby vycházejí z postavení ČP coby provozovatele ISDS [zákon č. 300/2008 Sb.; §14, odst. 2]. Osobní údaje, které jsou zpracovávány v rámci aplikace, jichž se bude penetrační test týkat, pocházejí z ISDS, které jsou v omezeném rozsahu vedeny ve veřejném Seznamu datových schránek (dále jen "SDS") [zákon č. 300/2008 Sb.; §14b, odst. 1, 3 a 5], a to včetně údajů fyzických osob, pokud tyto nepožádaly, aby jejich údaje byly v SDS zlikvidovány [zákon č. 300/2008 Sb., §14b, odst. 4]. Datové schránky těch fyzických osob, které o zlikvidování požádaly, smějí být vyhledatelné jen ze strany orgánu veřejné moci (nebo jiných subjektu, kterým fyzické osoby údaj samy sdělily a daly svůj souhlas k jejich zpracování). V dotčené webové aplikaci ČP, která je předmětem penetračního testu, to má vztah k předvyplňování objednávek.

Aplikace umožňuje dobíjení kreditu datových schránek, a umožňuje zasílání poštovních datových zpráv v případech, kdy odměnu hradí odesílatel. V rámci přímého přístupu do aplikace je možnost anonymního nabíjení a tento přístup je předmětem penetračního testu. Druhou možností je úhrada je kreditu, jenž je nakupován pres webovou aplikaci ISDS a zde je předáváno ID DS ze které je uživatel do aplikace pro dobíjení kreditu přistupuje. Tento proces není předmětem penetračního testu a nelze jej v rámci testovacího prostředí ani simulovat jak je uvedeno níže.

Zpracování osobních údajů v obou testovaných aplikacích se dále řídí ustanoveními zákona o ochraně osobních údajů [zákon č. 110/2019 Sb.].

Tato webová aplikace ČP, která je předmětem penetračního testu, není kategorizována podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti ani nepodléhá zákonu č. 240/2000 Sb., o krizovém řízení. Přesto ČP do role etalonu bezpečnosti implementuje relevantní požadavky specifikované ve vyhlášce pro všechny informační systémy (dále jen „IS“) Objednatele z důvodu uplatnění interního standardu. Jedná se především o §22, §25, §26 a §27 vyhlášky o kybernetické bezpečnosti.

3. Aplikace

Webová aplikace, která bude podrobena penetračnímu testu, přímo nespadá do fyzického perimetru ISDS, ale významně ovlivňuje bezpečnost uživatelů ISDS. Ověření bezpečnosti ISDS není přímo cílem tohoto penetračního testu. Cílem penetračního testu je aplikace pro dobíjení kreditu, která může významně ovlivnit ochranu informací držitelů DS, a to přesto, že je provozována mimo fyzický perimetr ISDS, jehož je ČP provozovatelem. To platí i pro níže popsané redirekce, které použije uživatel, když

dobíjí kredit pro PDZ nebo DT po přihlášení do klientského portálu (dále jen "KP") ISDS a dělá to tedy z webových stránek ISDS.

Webová aplikace, která bude testována, poskytuje ČP ze své vlastní aplikační infrastruktury. A tato (a další) aplikace má svůj vlastní doménový kontext.

Aplikace "Kreditní systém datových schránek"

Jedná se o webovou aplikaci ČP pro dobíjení kreditu za účelem posílání PDZ:

Testovací aplikace je umístěna v interním prostředí ČP a není přístupná z Internetu. Testovací prostředí bude Dodavatele zpřístupněno pomocí VPN a je dostupné na adrese https://www.test.kredit-ds.cz

Produkční prostředí je, respektive bude přístupné na adrese www.kredit-ds.cz (prozatím je tam provozována původní aplikace).

Tato aplikace bude volně přístupná i z internetu, bez autentizace. Uživatel tedy nemusí být přihlášen do ISDS ani jiné aplikace. V takovém případě se provádí ověření existence ID datové schránky (dále jen "DS"), které sám zadá. Pokud je uživatel právě přihlášen do klientského portálu (dále jen "KP") ISDS, a rozhodne se dobít kredit v rámci tohoto KP ISDS, je z něj přesměrováván vždy do kreditní aplikace ČP. To platí jak pro případ, kdy chce dobíjet kredit pro PDZ, tak i pro případ, kdy chce dobíjet kredit pro DT. Tehdy, protože jde z KP ISDS do kterého je už přihlášen, je mu předvyplněno ID DS a nemusí ho zadávat. Jestliže po přihlášení do KP ISDS dobíjí kredit pro PDZ, je do webové aplikace ČP pro dobíjení kreditu přesměrován ze zdrojového URL:

https://www.mojedatovaschranka.cz/portal/ISDS/nastaveni/pdz/odesilani

Chce-li však po přihlášení do KP ISDS dobíjet kredit pro účely DT (v tomto případě je minimálním počtem 20 zpráv, maximem je 5000 zpráv; datum aktivace nezadává, bere se vždy aktuální), je do téže webové aplikace ČP pro dobíjení kreditu přesměrován ze zdrojového URL:

https://www.mojedatovaschranka.cz/portal/ISDS/nastaveni/dudz/kredit/form/0

Cíl obou přesměrování je stejný, a to:

https://www.kredit-ds.cz/apdk_web/payment.html

Rovněž požadavek, který odejde z KP ISDS, je v obou výše uvedených případech totožný:

GET /apdk_web/payment.html?dsId={idds}&isds=true HTTP/1.1

Host: www.kredit-ds.cz

Pokud chce uživatel ISDS dobíjení provádět, bez přihlášení do KP ISDS, musí k tomu použít kreditní aplikaci ČP, pak tedy pres internet přistoupí do domény:

www.kredit-ds.cz. V rámci této aplikace tedy může uživatel dobít kredit libovolné DS.

V takovém případě muže do webové aplikace přijít jak protokolem HTTP (s přesměrováním na protokol HTTPS, které provede zařízení ČP) nebo rovnou protokolem HTTPS. Z domovské

stránky aplikace je přesměrován vždy na URL:

https://www.kredit-ds.cz/apdk_web/payment.html, kde provede vložení ID DS, zadá svůj potvrzovací e-mail (je použit pro doručení daňového dokladu, není-li tento posílán do DS a připadne pro pozdější urgenci platby, pokud byla zvolena platba přes banku, ale nebyla následně provedena), částku pro dobití, způsob platby, odsouhlasí obchodních podmínek ČP a rozhodne se, zda chce daňový doklad poslat do své DS.

Dalším krokem je přesměrování na platební bránu, kde provede platbu a pokud se nerozhodne jinak, bude poté vrácen zpět do aplikace ČP.

Poznámka: Má-li DS dobitý kredit pro PDZ, muže případně dotovat odesílání PDZ jiné datové schránce (Toto platí pouze pro ty, co mají smluvní formu PDZ. Nikoliv pro kredit). Tato funkce je interním mechanismem ISDS a tudíž v rámci tohoto penetračního testu nebude ověřována. Ve vztahu k ISDS také platí, že penetrační tester nebude ověřovat redirekce z příslušných stránek KP ISDS, tj. ty, které vedou po přihlášení z KP ISDS do webové aplikace ČP. Odkazy, které jsou umístěny pro PDZ za tlačítkem "DOBÍT KREDIT" a pro aktivaci či dobití kreditu u DT za tlačítkem "DOBÍJENÍ KREDITU" v prostředí Veřejného testu ISDS, totiž neprovádějí redirekci, ale rovnou připíší virtuální kredit pro účely testování uvnitř ISDS.

4. Metodika

Objednatel požaduje, aby byly penetrační testy provedeny v souladu s metodikou The Open Worldwide Application Security Project (dále jen "OWASP") Web Security Testing Guide (dále jen "WSTG"). Aktuální verze v čase zadání penetračního testu je 4.2 (uvolněna byla 3. prosince 2020). Nachází se na adrese https://github.com/OWASP/wstg. Spolu s tím zohlední penetrační

test také doporučenou bezpečnostní praxi, alespoň v rozsahu:

- OWASP Cheat Sheets (https://github.com/OWASP/CheatSheetSeries/tree/master/cheatsheets);
- W3C Content Security Policy Level 2 (https://www.w3.org/TR/CSP2/);
- W3C Cross-Origin Resource Sharing (https://www.w3.org/TR/2020/SPSD-cors-20200602/);
- Fetch API Living Standard (https://fetch.spec.whatwg.org/);
- HTML Living Standard (https://html.spec.whatwg.org/).

V potaz budou brány také relevantní RFC (jako např. RFC 2616, RFC 7540, RFC 6454, RFC 3986, RFC 5246 a další) připadající z povahy věci v úvahu pro testované aplikace (zejména

pak sekce "Security Considerations", které jsou v RFC obsaženy).

Penetrační tester také ověří, zda se v aplikaci nacházejí zvenčí detekovatelné technické zranitelnosti (např. zastaralé verze produktu se známými zranitelnostmi), ať už by měly dopad na uživatele aplikace nebo by mely dopad na ČP. Ověřovány budou jak zranitelnosti s dopadem na klientské straně (např. cross-site scripting, clickjacking, open redirekce či jiné útoky vedené proti klientovi), tak i zranitelnosti na serverové straně (např. command injection, open relay, server side request forgery nebo remote code execution proti webovému či aplikačnímu serveru).

Penetrační test nebude zahrnovat kontrolu technických zranitelností serverového operačního systému a jeho zodolnění, které si ČP kontroluje vlastními prostředky v interní síti.

Poznámka: Kreditních aplikace nespadá pod Payment Card Industry Data Security Standard (PCI DSS) a nebude podle něj testována. Externí funkce platební brány, kterou aplikace využívají, už nespadají do rozsahu penetračního testu.

Penetrační test rovněž nebude zahrnovat specifické ověřování odolnosti webových aplikací proti útokům zaměřeným na odepření služeb (DoS) jako jsou např. TCP/UDP -ood, útoky proti DNS, HTTP -flood, útoky pomocí slow technik, fragmentací apod. To ale neznamená, že aplikační zranitelnosti, které by vedly k nekontrolovatelné spotřebě zdrojů (jako je např. CWE-400), k exponenciálně složitým výpočtům či výkonově náročným aplikacím zpracováním (jako je kupř. CWE-1333), jsou mimo rozsah penetračního testu. Zranitelnosti aplikací nebo aplikační infrastruktury s dopadem na dostupnost služeb penetračnímu testu podléhají.

V rámci penetračních testu bude kromě jiného provedena také kontrola bezpečnostních nastavení firewallu, ale i bezpečnosti domény a vlastností TLS certifikátu (jako např. DNS Certification Authority Authorization nebo Certicate Transparency), konfigurace TLS protokolů, výměn, vlastností šifrovacích sad a klíčů, využití Strict-Transport-Security včetně preloadingu, prosazení Perfect-Forward Secrecy, kontrola výskytu známých zranitelností TLS (jako BEAST, POODLE, DROWN, ROBOT a další), kontrola bezpečnostních HTTP hlaviček a dalších mechanismu tohoto druhu, které ovlivňují bezpečnost aplikace, ať už na straně domény, serveru nebo klienta (jako jsou např. direktivy CSP2).

Pro vyhledávání zranitelností muže penetrační tester použít i automatizované nástroje (skener zranitelností). Takový nástroj ale má mít jen doplňkovou roli, aby snížil pracnost, usnadnil fázi sběru informací o aplikaci, zjednodušil mapování aplikačních cílů a tak podobně. Penetrační test se nesmí omezit jen na schopnosti takových nástrojů ani na jejich přesnost (ve smyslu nedotažení nejistých zjištění, ne zcela prokázaných podezření nebo případných false positives nálezu). Požadujeme, aby penetrační test prováděl kvalifikovaný tester, s dostatečnou zkušeností s podobnými aplikacemi, znalý i manuálních postupu, které jsou zapotřebí k dostatečné kvalitní simulaci aktivit zkušeného a schopného útočníka, který by se na aplikaci konkrétně zaměřil a věnoval jí úsilí, ne ji jen automatizované skenoval. Ruční testování bude tvořit hlavní část testovacího procesu a skenování automatizovanými nástroji muže být minoritní, doplňkovou částí, použitou tam, kde jde o rutinní práci, která by byla manuálně neefektivní. Připadne muže výsledek automatizovaného skenu sloužit jako podklad pro další ruční prověření.

Detailní zpráva, jak je popsána v následující kapitole, nebude generována automatickým skenerem. Tam, kde bude možné z jednotlivých zjištění sestavit navazující řetězec, kde jeden nález půjde spojit s dalšími nálezy a jejich komplet pak bude tvořit další, závažnější zranitelnosti, to penetrační tester vzájemně propojí, vyhodnotí a popíše.

Penetrační test nebude řešit shodu webové aplikace s legislativou, která se týká ISDS (jmenovité zákona č. 300/2008 Sb. a jeho prováděcí vyhlášky), ve věci poskytovaných služeb PDZ a DT či úhrady za ně. Objednatel nepožaduje, aby penetrační test posuzoval shodu se zákony regulujícími elektronický obchod či reklamu (např. zákon č. 480/2004 Sb. a další normy v této oblasti). Nicméně, penetrační test se bude zabývat shodou zpracování osobních údajů v této aplikaci legislativou. Ověří, zda některé aspekty zpracování osobních údajů nejsou u DS fyzických osob v neshodě s platnými ustanoveními zákona č. 300/2008 Sb. (správce ISDS provozovateli vyložil, že zveřejňované údaje nesmí překračovat rozsah zveřejňovaný v SDS) nebo zákona č. 110/2019 Sb., resp. evropského nařízení GDPR.

5. Organizace

Před realizací penetračního testu bude proveden společný workshop s Dodavatelem, na kterém Objednatel předá vybranému penetračnímu testerovi informace o testovacím prostředí, odprezentuje mu funkcionalitu aplikace a předá mu dostupnou aplikační dokumentaci. V rámci workshopu Objednatel předá penetračnímu testerovi přístupy do VPN (viz kap. 6) a URL aplikací v interním testovacím prostředí, aby měl možnost se s webovými aplikacemi následně seznámit a aby mohl získané informace použít při přípravě plánu.

Penetrační tester předloží do 1 týdne od vystavení objednávky plán testu, který obsáhne fáze testu, jeho přípravu, provedení, předložení zprávy, její vypořádání, součinnost (vč. eskalačních kontaktu) a pro test použité nástroje. Po schválení plánu ze strany Objednatele bude penetrační test zahájen.

Předpokládané zahájení penetračního testu bude k datu do 14 dní od účinnosti Smlouvy a trvání penetračního testu bude nejvýše 2 týdny. Zahájení a trvání následných retestu bude upřesněno dle toho, jaká budou zjištění, kolik jich bude a jaký čas bude zapotřebí k nasazení oprav a jejich retestům (případně také dle toho, zda bude možné provést všechny retesty v testovacím prostředí, nebo bude nutné některé skutečnosti doprověřit i v produkčním prostředí, až po nasazení aplikace – viz upozornění na konci této kapitoly).

Rozsah webové aplikace není takový, aby musely být po částech předkládány dlíčí zprávy. Dodavatel předloží jednu detailní zprávu a v ní se bude postupně věnovat zjištěným nálezům.

Pro každé zjištění, které bude ve zprávě popsáno, uvede penetrační tester tyto údaje:

- cíl, kde se zjištění vyskytuje (pokud je specifický a zjištění neplatí pro aplikaci obecně)
- povaha zjištění (např. cross-site scripting, otevřená redirekce atd.);
- popis zjištění (v čem bezpečnostní zranitelnost spočívá, jaké jsou její příčiny – zda spočívají v návrhu nebo v implementaci, jaké jsou předpoklady a podmínky či scénáře jejího odhalení a/nebo následného zneužití, případně vazby na jiné zranitelnosti, které byly rovněž zjištěny);
- důkaz zjištění (např. ukázka odeslaného požadavku a vrácené odezvy či jiná, vhodná formu důkazu jako je případně výsledek skenu konfigurace apod.)
- bezpečnostní dopady (ať už mířící na uživatele ČP, na externí na platební bránu nebo na vlastní webovou aplikaci ČP a její infrastrukturu);
- závažnost dopadu (na stupnici 1 - nízká, 2 - střední, 3 - závažná, 4 - kritická);
- klasifikace zranitelnosti dle Common Weakness Enumeration (https://cwe.mitre.org/), zvláště je potřebné uvést, půjde-li o některou zranitelnosti z CWE Top 25;
- klasifikace zranitelnosti dle OWASP Top 10 (https://owasp.org/Top10/), pokud o takovou zranitelnost půjde;
- identifikace zranitelnosti dle Common Vulnerabilities and Exposures (jen u technických zranitelností produktu);
- doporučení k nápravě nebo eliminaci dopadu zranitelnosti (musí být natolik konkrétní, aby podle nej mohl při opravě postupovat vývojář, v případě technických zranitelností by mělo být uvedeno, zda je nutné komponentu úplně vyměnit nebo povýšit její verzi na konkrétní, nezranitelnou).

V závěru zprávy budou sepsána souhrnná doporučení penetračního testera sledující nejen nápravu jednotlivých zranitelností, ale zejména další zdokonalení celkové bezpečnosti testovaných aplikací.

Penetrační tester bude detailní zprávu a jednotlivá zjištění či nálezy z ní podrobně prezentovat a vysvětlovat na společném workshopu, které k tomu s dalšími dotčenými pracovníky ČP (vývojáři, architektura, provoz, ochrana osobních údajů, gestory aj.) svolá projektová manažer ČP. Účelem workshopu bude zajistit, že zjištění budou natolik dobře vyložena a vyargumentována a jejich příčiny budou tak podrobně vysvětleny, aby ten, kdo je bude řešit, získal dostatečnou informaci o tom, co konkrétně a proč má být opraveno i jak bude poté oprava ověřena. V případě potřeby bude penetrační tester připraven poskytnout vybraným řešitelům i další individuální telefonickou či online konzultaci nebo e-mailem odpovědět na doplňkové dotazy, pokud takové vzniknou.

Součástí penetračních testu budou dvě kola následných retestů, v jejichž průběhu penetrační tester potvrdí, zda ČP dostatečné odstranila nebo neodstranila zjištěné zranitelnosti a vyhodnotí zbytkovou závažnost dopadu u těch zranitelností, jejichž nápravu posoudí jen jako částečnou. Penetrační tester na závěr zpracuje souhrnnou zprávu.

Upozornění: V ČP se muže stát, že vlastnosti interního testovacího prostředí se nemusejí zcela shodovat s produkčním prostředím, ve kterém je nakonec webová aplikace publikována do internetu. Penetrační tester proto musí počítat s tím, že závěrečné, druhé kolo retestu muže pro některá zjištění provádět i proti produkčnímu prostředí pres internet. Zda k tomu dojde, o tom rozhodne povaha zjištění. V případě, že finální retest bude i proti produkčnímu prostředí, bude při něm penetrační tester postupovat tak, aby nevznikla škoda třetím stranám nebo to nepoškodilo jiné aplikace ČP. U zjištění, kde by toto nebylo možné garantovat, na to penetrační tester ČP předem upozorní a ČP pak rozhodne, zda budou dotčená zjištění z posledního kola retestu vyloučena.

6. Součinnost

ČP určí aplikační cíle (URL), poskytne přístup do testovacího prostředí, vyloží funkcionalitu aplikací, předá dostupnou aplikační dokumentaci a jmenuje kontaktní a eskalační pracovníky na své straně. Hlavní penetrační testování bude prováděno před publikováním aplikace v produkčním prostředí. ČP poskytne testovací prostředí, zajistí jeho připravenost a neměnnost (jak aplikačního, tak i běhového prostředí) v průběhu penetračního testu. Přístup do testovacího prostředí bude realizován pomocí VPN. Bude použit klient Cisco AnyConnect. ČP poskytne pro penetrační test vlastní VPN i dostatečnou přenosovou kapacitu. Bude-li potřebné zajistit, aby měl penetrační tester připojený do VPN k dispozici také externí zdroje (např. testovací platební bránu), zvolí ČP takovou konfiguraci (VPN split), která to dovolí. Penetrační tester musí v plánu včas upozornit na to, zda by prvotní nastavení VPN (bez splitu, které dostal pro přípravu plánu) nepostačovalo pro test.

Dodavatel penetračního testu jmenuje kvalifikované, profesně zdatné a zkušené pracovníky, kteří budou vykonávat penetrační testy. Pro přístup do VPN je nezbytné:

- registrovat penetrační testery v systému řízení identit ČP;
- předat ČP osobní údaje penetračních testerů v rozsahu: jméno, příjmení, firma, e-mail a mobilní telefon;
- penetrační tester si zajistí komerční přístupový (nikoliv testovací) certifikát vydaný CA PostSignum (ČP k tomu předá relevantní počet voucheru platných po dobu 1 roku);
- penetrační testeři si na počítacích, odkud budou penetrační test provádět, nainstalují a nastaví klientskou aplikaci Cisco AnyConnect;

Upozornění: Na pracovních stanicích penetračních testeru bude zajištěna potřebná úroveň bezpečnosti, bude zde instalován antivirus a osobní firewall a budou správně konfigurovány či udržovány. Penetrační testeři nebudou v interním prostředí ČP používat neschválené a neprověřené penetrační nástroje (např. kompilované GNU nástroje za jejichž pravost a skutečnou funkčnost se dodavatel penetračního testu neumí zaručit). Pokud by vyvstala potřeba použít nástroje, se kterými plán nepočítal, smí k tomu dojít až po souhlasu ze strany ČP.

7. Výstupy

1) Návrh penetračních testů - libovolná struktura
2) Provedení penetračních testů
3) Detailní závěrečná zpráva s jednotlivými zjištěními či nálezy
4) Workshop pro prezentaci závěrečné zprávy, který zajistí:
    a. že zjištění budou správně pochopena dobře vyložena a vyargumentována,
    b. jejich příčiny budou podrobně vysvětleny
    c. konzultaci s vývojáři ČP v rozsahu 4 hod.
5) Retest penetračních testů – předpokládáme provedení jednoho nebo dvou retestů (nacenit jeden retest)

Cena

Sazba (cena) za 1 člověkoden (MD)[1] v Kč bez DPH	7 500,00
Počet člověkodní za návrh a provedení penetračních testů	12
Počet člověkodní za provedení jednoho (1) retestu penetračních testů	2
Maximální celkový počet člověkodní alokovaných pro předmět plnění této Smlouvy[2]	16
Maximální celková cena za Plnění v Kč bez DPH	**120 000,00**

[1] Jedním člověkodnem (MD) se rozumí 8 hodin výkonu práce jednoho pracovníka Dodavatele pro Objednatele.

[2] Do maximálního počtu člověkodní alokovaných pro předmět plnění této Smlouvy je zahrnuto provedení dvou (2) retestů penetračních testů. Cena bude hrazena dle skutečně provedených retestů.

Příloha č. 2: Složení realizačního týmu Dodavatele

Realizační tým Dodavatele bude složen z následujících členů:

jméno a příjmení	role (pozice) v realizačním týmu
[redacted]	manažer zakázky
[redacted]	auditor
[redacted]	konzultant