RÁMCOVÁ SMLOUVA

Penetrační testy aplikací TCPK

uzavřená níže uvedeného dne, měsíce a roku podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů

Čl. 1. Smluvní strany

1.1. Plzeňský kraj

se sídlem: Škroupova 18, 306 13 Plzeň
IČ: 70890366
DIČ: CZ 70890366
zastoupený: Václavem Šlajsem, hejtmanem Plzeňského kraje
na základě Podpisového a kompetenčního řádu Plzeňského kraje a Krajského úřadu Plzeňského kraje k podpisu oprávněn Mgr. Jiří Leščinský, ředitel, Krajský úřad Plzeňského kraje
bankovní spojení: Raiffeisenbank a.s., pobočka Plzeň
č.ú.: 1083003606/5500
kontaktní osoba: Ing. Jiří Lohr, vedoucí oddělení správy serverů a sítě, odbor informatiky KÚPK
telefon: +420 377 195 207
e-mail: jiri.lohr@plzensky-kraj.cz
(dále jen „objednatel“, „zadavatel“)

a

1.2. Corpus Solutions a.s.

se sídlem / místem podnikání: Na Vítězné pláni 1719/4, 140 00 Praha 4
IČ: 25764616
DIČ: CZ25764616
zastoupený/jednající: Ing. Tomášem Přibylem, předsedou představenstva
bankovní spojení: Raiffeisenbank a.s.
č.ú.: 69474001/5500
zapsán v obchodním rejstříku, vedeném Městským soudem v Praze, oddíl B, vložka č. 5936
kontaktní osoba: Ondřej Pilát, manažer pro klíčové zákazníky
telefon: +420 736 609 363
e-mail: ondrej.pilat@corpus.cz
(dále jen „dodavatel, poskytovatel“)

Čl. 2. Úvodní ustanovení

2.1.1. Tato smlouva je uzavírána v návaznosti na veřejnou zakázku malého rozsahu s názvem „Penetrační testy aplikací TCPK“, zadávanou objednatelem jakožto zadavatelem.

2.1.2. Cílem uzavřené smlouvy je poskytování definovaných služeb penetračních testů na základě dílčích objednávek poskytovatelem objednateli za řádně smluvenou cenu.

2.1.3. Základní metodikou pro provádění penetračních testů je metodika OWASP (www.owasp.org - Open Web Application Security Project).

2.1.4. Cílem provádění penetračních testů je odhalení zranitelností aplikací nasazených Plzeňským krajem v jeho technologickém centru a na základě zjištění těchto zranitelností jejich odstraňování a tím zvyšování bezpečnosti takových aplikací.

2.1.5. V rámci plnění této smlouvy budou realizovány i penetrační testy aplikací realizovaných v projektech Plzeňského kraje v rámci Výzvy č. 08 na „Rozvoj služeb eGovernmentu v krajích“ Integrovaného operačního programu (IOP) a to projektů:

- **Digitální mapa veřejné správy Plzeňského kraje** – část II

  CZ.1.06/2.1.00/08.07276 (dále se bude používat zkratka „DMVS“)

- **ICT služby technologického centra Plzeňského kraje** – části I, III, IV a V

  CZ.1.06/2.1.00/08.07231 (dále se bude používat zkratka „ICTS“)

- **Technologické centrum Plzeňského kraje** – část VI

  CZ.1.06/2.1.00/08.07277 (dále se bude používat zkratka „TCPK“)

Čl. 3. Předmět smlouvy

3.1.1. Předmětem smlouvy je poskytování úplatných služeb

- Prvního penetračního testu,
- Opakovaného penetračního testu
- a Individuálních zranitelností

definovaných v příloze č. 1 této smlouvy – Technické dokumentaci na základě dílčích objednávek. Dále jen („penetrační testy“ nebo „testy“).

3.1.2. Objednatel předpokládá rozsah věnovaný testování jedné aplikace, tj. První penetrační test nebo Opakovaný penetrační test, v rozsahu 3-4 pracovních dnů kvalifikovaným dodavatelem.

3.1.3. Objednatel předpokládá náročnost na prokázání jedné Individuální zranitelnosti 0,5 člověkodne.

3.1.4. Služby budou realizovány v souladu s Technickou dokumentací a s Metodikou přístupu poskytovatele, které jsou přílohami této smlouvy. V případě nesouladu těchto příloh má přednost příloha č. 1 smlouvy - Technická dokumentace.

3.1.5. Součástí předmětu plnění jsou i práce v tomto článku smlouvy nespecifikované, které však jsou k řádnému provádění rozvoje nezbytné a o kterých dodavatel vzhledem ke své kvalifikaci a zkušenostem měl, nebo mohl vědět. Provedení těchto prací však v žádném případě nezvyšuje touto smlouvou sjednanou cenu rozvoje.

Čl. 4. Cena a platební podmínky

4.1.1. Cena za služby penetračních testů představuje nabídkovou cenu předloženou dodavatelem v jeho nabídce na veřejnou zakázku „Penetrační testy aplikací TCPK“.

4.1.2. Objednatel a dodavatel se dohodli, že

A) cena za jeden „První penetrační test“ činí **9.000,-** Kč bez DPH,

B) cena za jeden „Opakovaný penetrační test“ činí **4.800,-** Kč bez DPH

C) a cena za prokázání jedné „Individuální zranitelnosti“ činí **4.000,-** Kč bez DPH.

4.1.3. Tato cena za jednotlivou službu je stanovena jako cena konečná a úplná.

4.1.4. Dodavatel není oprávněn požadovat po dodavateli poskytnutí zálohy.

4.1.5. Dodavatel na sebe bere odpovědnost za to, že sazba a výše daně z přidané hodnoty bude stanovena v souladu s platnými právními předpisy.

4.1.6. Daň z přidané hodnoty bude připočtena k ceně za službu ve výši dle právní úpravy platné ke dni uskutečnění zdanitelného plnění.

4.1.7. Sjednaná jednotková cena za služby uvedená v článku 4.1.2 této smlouvy je cenou nejvýše přípustnou, kterou je možné překročit pouze v případě zvýšení sazby DPH, a to tak, že dodavatel ke sjednané ceně bez DPH připočítá DPH v procentní sazbě odpovídající zákonné úpravě účinné k datu uskutečnitelného zdanitelného plnění.

4.1.8. Cena za služby bude hrazena na základě faktur vystavených dodavatelem.

4.1.9. Faktury na zaplacení sjednaných cen je dodavatel oprávněn vystavit nejdříve následující den po dni obdržení potvrzení o provedené akceptaci penetračního testu od kontaktní osoby objednatele.

4.1.10. V případě neprokázání „Individuální zranitelnosti“ dle přílohy č. 1 smlouvy – Technické dokumentace není dodavatel oprávněn požadovat úplatu a není oprávněn vystavit na takové plnění fakturu.

4.1.11. Splatnost faktur činí 30 dnů ode dne jejich prokazatelného doručení na adresu sídla objednatele.

4.1.12. Faktura bude mít náležitosti daňového dokladu dle platných právních předpisů (zákona č. 563/1991 Sb., o účetnictví, v platném znění a zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění).

4.1.13. Faktury musí obsahovat název smlouvy, číslo účtu dodavatele a všechny údaje uvedené v § 28 odst. 2 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.

4.1.14. V případě, že faktura – daňový doklad nebude obsahovat stanovené náležitosti nebo v něm nebudou správně uvedené údaje, je objednatel oprávněn ji vrátit ve lhůtě splatnosti zpět dodavateli s uvedením chybějících náležitostí nebo nesprávných údajů. V takovém případě přeruší běh lhůty splatnosti a nová lhůta splatnosti počne běžet doručením opravené faktury – daňového dokladu.

4.1.15. Po vzniku práva fakturovat je dodavatel povinen vystavit a objednateli předat fakturu.

4.1.16. Cena bude dodavateli zaplacena bezhotovostní formou převodem na jeho bankovní účet. Faktura je považována za proplacenou okamžikem odepsání příslušné částky z účtu objednatele ve prospěch účtu dodavatele.

4.1.17. Dodavatel souhlasí s tím, aby subjekty oprávněné dle zák. č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, provedly finanční kontrolu závazkového vztahu vyplývajícího ze smlouvy s tím, že se dodavatel podrobí této kontrole, a bude spolupůsobit jako osoba povinná ve smyslu ust. § 2 písm. e) uvedeného zákona při výkonu finanční kontroly prováděné v souvislosti s úhradou služeb z veřejných výdajů.

4.1.18. Každý originální účetní doklad vztahující se k penetračnímu testu aplikace z projektu Výzvy č. 08 bude obsahovat informaci, že se jedná o projekt IOP a musí být označen číslem projektu.

4.1.19. Pokud to bude možné, bude účetnictví vedeno v elektronické formě. V souladu s předpisy ES se účetní záznamy o účetních operacích budou v co největší možné míře uchovávat v elektronické formě, minimálně do 31.12.2021.

4.1.20. Dodavatel se zavazuje řádně uchovávat veškerou dokumentaci související s realizací předmětu smlouvy, včetně účetních dokladů v souladu s článkem 90 Nařízení Rady (ES) č. 1083/2006 minimálně do konce roku 2021, pokud zvláštní právní předpis nestanoví v době trvání tohoto závazku zhotovitele lhůtu delší.

4.1.21. Dodavatel je povinen všechny písemné zprávy, písemné výstupy a prezentace týkající se penetračních testů aplikací z projektů IOP Výzvy č. 08 opatřit vizuální identitou projektů dle Pravidel pro provádění informačních a propagačních opatření (viz příloha č. 4 Příručky).

4.1.22. Dodavatel prohlašuje, že ke dni nabytí účinnosti této smlouvy je s těmito pravidly seznámen. V případě, že v průběhu plnění této smlouvy dojde ke změně těchto pravidel, je zadavatel povinen o této skutečnosti zhotovitele bezodkladně informovat.

Čl. 5. Doba trvání smlouvy

5.1.1. Smlouva se uzavírá na dobu neurčitou s platností a účinností ode dne jejího uzavření oběma smluvními stranami.

5.1.2. Objednatel i poskytovatel jsou oprávněni tuto smlouvu vypovědět, a to na základě písemné výpovědi, prokazatelně doručené druhé smluvní straně. Výpovědní lhůta činí 2 kalendářní měsíce a začíná běžet od prvního dne kalendářního měsíce následujícího po měsíci, v němž byla výpověď doručena druhé smluvní straně.

Čl. 6. Místo plnění:

6.1.1. Místem poskytování služeb je sídlo objednatele na adrese Škroupova 18, Plzeň.

6.1.2. Za účelem provádění služeb na základě této rámcové smlouvy bude s dodavatelem uzavřena samostatná smlouva o vzdáleném přístupu k HW a SW prostředí jednotlivých aplikací objednatele.

Čl. 7. Maximální rozsah plnění a garantovaný odběr plnění

7.1. Maximální rozsah plnění

7.1.1. Na základě této smlouvy mohou být odebrány služby uvedené v předmětu smlouvy v součtu maximálně do výše 1.960.000,- Kč bez DPH.

7.2. Garantovaný odběr plnění

7.2.1. Objednatel garantuje dodavateli odebrání 10 služeb „Prvního penetračního testu“ v prvních 2 letech od uzavření smlouvy, když objednávka služeb „Opakovaného penetračního testu“ a „Individuální zranitelnosti“ je odvislá od výsledků „Prvního penetračního testu“ jednotlivé aplikace.

Čl. 8. Realizace poskytování služeb, práva a povinnosti smluvních stran

8.1. Objednávka poskytnutí služeb penetračních testů

8.1.1. K podávání objednávek za objednatele a k příjmu objednávek za dodavatele jsou oprávněny kontaktní osoby na základě této smlouvy.

8.1.2. Součástí objednávky bude vždy uvedení:

A) požadovaného typu služby,

B) určení aplikace pro testování s jednoduchým popisem aplikace a údaji potřebnými pro přístup k aplikaci

C) a datum vystavení této objednávky.

8.1.3. Objednávka je považována za vystavenou dnem jejího odeslání emailem kontaktní osobou objednatele.

8.1.4. V případě potřeby testování aplikace formou vzdáleného přístupu zajistí vzdálený přístup pro dodavatele kontaktní osoba objednatele současně s podáním objednávky na základě této smlouvy.

8.2. Přijetí objednávky a návrh termínů realizace testů

8.2.1. Kontaktní osoba dodavatele potvrdí kontaktní osobě objednatele nejpozději do 5 pracovních dnů přijetí objednávky a současně navrhne termíny provedení testů.

8.2.2. V případě potřeby objednatele na doplnění dalších relevantně potřebných informací k řádnému provedení služby testů je kontaktní osoba dodavatele oprávněna si takové informace vyžádat ve lhůtě pro potvrzení přijetí objednávky dle ustanovení článku 8.2.1. této smlouvy.

8.2.3. Penetrační testy bude možné provádět výhradně mimo hlavní část pracovní doby v pracovním týdnu, tj. mimo hodiny 08:00 až 15:00 v pracovním týdnu.

8.2.4. Provádění penetračních testů v pracovních dnech v hodinách od 08:00 do 15:00 hodin, je možné pouze za písemného udělení výjimky kontaktní osobou objednatele.

8.2.5. Kontaktní osoba objednatele do 2 pracovních dnů od obdržení navrhovaných termínů potvrdí objednateli vybraný termín realizace testů, doplní případné vyžádané relevantní potřebné informace pro provedení testů.

8.3. Termíny realizace penetračních testů

8.3.1. „První penetrační test“ a „Opakovaný penetrační test“ je dodavatel povinen realizovat nejpozději ve lhůtě 1 kalendářního měsíce ode dne odeslání objednávky kontaktní osobou objednatele.

8.3.2. Test „Individuální zranitelnosti“ je dodavatel povinen realizovat nejpozději do 3 týdnů ode dne odeslání objednávky kontaktní osobou objednatele.

8.3.3. Termíny pro realizaci jednotlivých testů je možné prodloužit na základě písemné oboustranně potvrzené dohody mezi kontaktními osobami.

8.4. Průběh realizace penetračních testů

8.4.1. O zahájení i ukončení provádění testů je kontaktní osoba dodavatele povinna vždy informovat kontaktní osobu objednatele, a to vždy v okamžiku jejich zahájení a v okamžiku jejich ukončení v předem dohodnutých termínech.

8.4.2. V případě výpadku (nedostupnosti) testované aplikace nebo jejího poškození je kontaktní osoba dodavatele povinna bezprostředně kontaktovat kontaktní osobu objednatele. Kontaktní osoby jsou v takovém případě oprávněny dohodnout další postup takového testu a to včetně změn nebo prodloužení termínů.

8.5. Zpráva o penetračním testu

8.5.1. Zpráva o provedeném penetračním testu dle přílohy č. 1 smlouvy – Technické dokumentace definovaná dle jednotlivého typu penetračního testu musí být předána kontaktní osobě objednatele ve lhůtě 3 pracovních dnů od ukončení provádění testu, nejpozději však v termínu pro realizaci konkrétního typu penetračního testu.

8.5.2. Zpráva bude zaslána buď ve formátu PDF a bude elektronicky podepsána kontaktní osobou, nebo osobou oprávněnou jednat jménem či za dodavatele, nebo bude zaslána v listinné podobě s podpisem kontaktní osoby nebo osoby oprávněné jednat jménem či za dodavatele. Zároveň dodavatel předá objednateli zprávu v dále zpracovatelném formátu (RTF), případně v jiném editovatelném formátu, který si obě smluvní strany odsouhlasí.

8.5.3. V případě zjištění zranitelnosti budou Zprávy o penetračních testech sloužit k prokázání těchto zranitelností dodavatelům aplikací za účelem zajištění jejich bezpečnosti.

8.6. Potvrzení (akceptace) realizovaného penetračního testu

8.6.1. Kontaktní osoba objednatele do 5 pracovních dnů ode dne doručení Zprávy o penetračním testu kontaktní osobě dodavatele

A) písemně potvrdí a akceptuje Zprávu o penetračním testu

B) nebo zašle připomínky a požadavky na dopracování a uvedení Zprávy o penetračním testu do souladu s touto smlouvou a zejména jejími přílohami č. 1 – Technickou dokumentací a č. 2 – Metodikou přístupu poskytovatele.

8.6.2. V případě potvrzení (akceptace) Zprávy o penetračním testu je dodavatel oprávněn následující den po doručení tohoto potvrzení vystavit fakturu za realizované plnění.

8.6.3. V případě obdržení připomínek a požadavků na dopracování a uvedení Zprávy o penetračním testu do souladu s touto smlouvou a zejména jejími přílohami č. 1 – Technickou dokumentací a č. 2 – Metodikou přístupu poskytovatele je dodavatel povinen provést nápravu do 5 pracovních dnů ode dne odeslání připomínek a požadavků od kontaktní osoby objednatele.

8.6.4. Proces připomínek a požadavků na dopracování Zprávy o penetračním testu může být opakován, vždy v termínu 5 pracovních dnů na vyjádření konkrétní kontaktní osoby smluvní strany, nedohodnou-li si kontaktní osoby termín jiný.

Čl. 9. Odstoupení od smlouvy

9.1.1. Smluvní strany jsou oprávněny od smlouvy ihned odstoupit v případě závažného porušení povinnosti vyplývající z této smlouvy druhou smluvní stranou. Odstoupení je účinné jeho doručením druhé smluvní straně.

9.1.2. Za závažné porušení povinnosti dodavatele se rozumí prodlení dodavatele s plněním povinností realizace služeb penetračních testů o více než 30 dní, pokud toto prodlení způsobil dodavatel, a odmítnutí provedení služeb penetračních testů, mimo výjimky u „Individuální zranitelnosti“ dle přílohy č. 1 smlouvy – Technické dokumentace.

9.1.3. Závažným porušením povinnosti objednatele se rozumí prodlení objednatele s úhradou faktur podle této smlouvy o více než 30 dní.

9.1.4. V případě odstoupení od smlouvy bude do 30 dnů provedeno vypořádání smluvních stran.

Čl. 10. Kontaktní osoby a projektový tým

10.1. Kontaktní osoby

10.1.1. Veškerá komunikace mezi smluvními stranami v záležitostech této smlouvy bude probíhat prostřednictvím kontaktních osob. Každá smluvní strana jmenuje kontaktní osobu. Každá ze smluvních stran má právo změnit jí jmenovanou kontaktní osobu, je však povinna vyrozumět o každé změně druhou smluvní stranu. Změna kontaktní osoby je vůči druhé straně účinná teprve okamžikem prokazatelného doručení takového vyrozumění.

Kontaktní osobou za objednatele je:

Ing. Jiří Lohr

Odbor informatiky

Krajský úřad Plzeňského kraje

email: jiri.lohr@plzensky-kraj.cz

telefon: +420 377 195 207

Kontaktní osobou za poskytovatele je:

Ondřej Pilát

Manažer pro klíčové zákazníky

Corpus Solutions a.s.

email: ondrej.pilat@corpus.cz

telefon: +420 736 609 363

10.1.2. Komunikace mezi kontaktními bude uskutečňována v elektronické podobě email nebo telefonicky.

10.1.3. Veškerá korespondence mezi smluvními stranami bude činěna v písemné formě a doručena druhé smluvní straně, přičemž písemná forma je zachována i v případě emailové zprávy.

10.1.4. Kontaktní osoby se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků. Kontaktní osoby jsou povinny informovat druhou smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této smlouvy.

10.2. Projektový tým

10.2.1. Dodavatel se zavazuje realizovat provádění jednotlivých penetračních testů tak, aby v každém týmu provádějícím testy byl zahrnut alespoň jeden z členů projektového týmu, které uchazeč předložil jako členy projektového týmu ve své nabídce na veřejnou zakázku.

10.2.2. Konkrétní složení projektového týmu pro jednotlivý test sdělí kontaktní osoba dodavatele kontaktní osobě objednatele bezprostředně po jeho vyžádání, nejpozději však do 2 pracovních dnů.

Čl. 11. Mlčenlivost a ochrana informací

11.1.1. V souvislosti s poskytování služeb penetračních testů na základě této smlouvy se smluvní strany zavazují zajistit utajení získaných důvěrných informací takovým způsobem, aby nemohlo dojít k jejich zneužití smluvní stranou nebo třetí osobou. Smluvní strany jsou zároveň povinny zajistit utajení získaných informací i u svých zaměstnanců, zástupců, jakož i spolupracujících třetích stran a osob.

11.1.2. Smluvní strany se výslovně dohodly, že pokud získají od druhé smluvní strany informace, o kterých vzhledem k povaze takových informací mohly předpokládat, že na jejich utajení má druhá smluvní strana oprávněný zájem anebo které nejsou v obchodních kruzích běžně dostupné (dále jen „důvěrné informace“), budou s těmito důvěrnými informacemi nakládat jako s vlastním obchodním tajemstvím, aniž by bylo nutné takové informace jako „důvěrné“ vždy jednotlivě označovat. Výše uvedené nevylučuje možnost v jednotlivých případech při zvýšeném zájmu toto označení pro jednotlivé informace použít.

11.1.3. Za důvěrné informace se bez ohledu na formu jejich zachycení považují rovněž veškeré informace, které nebyly některou ze stran označeny jako veřejné a které se týkají plnění smluvních a jinak dohodnutých povinností, které se týkají některé ze stran (zejména obchodní tajemství, know-how atd.), anebo informace, pro nakládání s nimiž je platnými

právními předpisy stanoven zvláštní režim utajení (zejména tajemství státní, hospodářské, bankovní, služební či ochrana osobních údajů).

11.1.4. Za důvěrné informace se dále považují takové informace, kterou jsou jako důvěrné výslovně kteroukoli ze smluvních stran označeny.

11.1.5. Smluvní strany jsou povinny zajistit utajení získaných důvěrných informací obvyklým způsobem, není-li výslovně sjednáno jinak. Tato povinnost platí bez ohledu na ukončení účinnosti této smlouvy. Strany jsou povinny zajistit utajení důvěrných informací i u svých zaměstnanců, zástupců, a i jiných spolupracujících třetích stran, pokud jim takové informace byly poskytnuty.

11.1.6. Porušení mlčenlivosti je považováno za závažné porušení smlouvy, na základě kterého je možné od smlouvy odstoupit.

Čl. 12. Smluvní pokuty

12.1.1. Pro případ prodlení se zaplacením řádně fakturované ceny se objednatel zavazuje dodavateli uhradit smluvní pokutu ve výši 0,01 % z fakturované ceny za každý den prodlení.

12.1.2. Za prodlení poskytovatele s poskytnutím součinnosti pro naplánování data realizace penetračního testu, se zahájením realizace penetračních testů v daných termínech a se zpracování Zprávy o provedeném penetračním testu se ustanovuje smluvní pokuta ve výši 1.000,- Kč za každý, byť jen započatý, den prodlení.

12.1.3. Pro každý zjištěný případ nedodržení složení projektového týmu se poskytovatel zavazuje objednateli uhradit smluvní pokutu ve výši 5.000,- Kč.

12.1.4. Pro každý zjištěný případ porušení mlčenlivosti a ochrany informací podle této smlouvy se ustanovuje smluvní pokuta ve výši 100.000,- Kč.

12.1.5. Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod, zejména s ohledem na předmět plnění smlouvy. Poskytovatel služeb jako odborník na problematiku penetračních testů je povinen dle této smlouvy upozornit na skutečnosti, které by mohli vést ke vzniku škody kontaktní osobu zadavatele. Upozornění jej však nezbavuje povinnosti maximálně předcházet škodám a jejich minimalizaci.

12.1.6. Zaplacením smluvní pokuty není dotčeno právo poškozené strany na náhradu škody.

12.1.7. Odstoupením od smlouvy se nedotýká nároku na zaplacení smluvní pokuty.

12.1.8. Žádná ze smluvních stran neodpovídá za škodu, která vznikla v důsledku věcně nebo jinak chybného zadání, které obdržel od druhé smluvní strany. Žádná ze stran není odpovědná za prodlení způsobené prodlením s plněním závazků druhé smluvní strany.

12.1.9. Výši smluvních pokut shodně považují obě smluvní strany za přiměřené. Smluvní pokuta je splatná do 30-ti dnů od doručení jejího vyúčtování.

Čl. 13. Závěrečná ustanovení

13.1.1. Smluvní strany se dohodly uzavřít smlouvu podle § 1746 odst. 2 zákona č. 89/2012 Sb., Občanského zákoníku, ve znění pozdějších předpisů.

13.1.2. Právní vztahy touto smlouvou výslovně neupravené a z ní vyplývající nebo s ní související se řídí příslušnými ustanoveními Občanského zákoníku.

13.1.3. Jakékoli změny či doplňky této smlouvy je možné platně učinit pouze formou písemných a vzestupně číslovaných dodatků, podepsaných oprávněnými zástupci obou smluvních stran.

13.1.4. Vzhledem k veřejnoprávnímu charakteru objednatele zhotovitel výslovně souhlasí se zveřejněním smluvních podmínek obsažených v této smlouvě v rozsahu a za podmínek vyplývajících z příslušných právních předpisů (zejména zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů).

13.1.5. Smlouva se pořizuje ve čtyřech (4) vyhotoveních s platností originálu, z nichž objednatel i dodavatel obdrží po podpisu každý dvě vyhotovení.

13.1.6. Tato smlouva nabývá platnosti a účinnosti dnem jejího uzavření.

13.1.7. Smluvní strany prohlašují, že smlouva byla sepsána dle jejich pravé a svobodné vůle, že si ji před jejím podpisem přečetly a s celým jejím obsahem souhlasí.

13.2. Přílohy smlouvy

- Příloha č. 1 smlouvy – Technická dokumentace
- Příloha č. 2 smlouvy – Metodika přístupu poskytovatele

V Praze dne 13.05.2014	V Plzni dne 06.05.2014
Za poskytovatele	Za objednatele
……	……
Ing. Tomáš Přibyl	**Mgr. Jiří Leščinský**
předseda představenstva	ředitel
Corpus Solutions a.s.	Krajský úřad Plzeňského kraje

Příloha č. 1 Rámcové smlouvy – Penetrační testy aplikací TCPK

Technická dokumentace zadavatele

Technická dokumentace veřejné zakázky malého rozsahu s názvem „Penetrační testy aplikací TCPK“

Čl. 1. Úvodní ustanovení

Tento dokument je určen k popisu a definici rozsahu služeb, které zadavatel poptává jako služby penetračních testů aplikací ve veřejné zakázce malého rozsahu s názvem „Penetrační testy aplikací TCPK.“

Čl. 2. Základní metodika pro provádění penetračních testů

2.1.1. Metodika provedení penetračních testů vychází z poznání, že nejlepší postup je v podstatě opakování určitých postupů, prováděných skutečnými útočníky. Tato metodika vychází z toho, že útočník postupně získává informace o cíli útoku, tyto informace upřesňuje a cíleně hledá a vylučuje slabiny cílového systému.

2.1.2. Objednatelem minimálně požadovaný postup je následující:

- **Identifikace cíle** – sběr informací o cíli, používaný rozsah IP adres, identifikace aktivních IP adres, detekce síťových služeb, operačních systémů a aplikací, výběr možných perspektivních cílů
- **Provedení automatických testů** – prostřednictvím různých specializovaných nástrojů, zjištění možných zranitelností, neinstalovaných bezpečnostních patchů a oprav, pokusy o prolomení vstupu do systému hrubou silou, pokusy o DOS útoky na aplikace. Detekce reakce cíle na útok.
- **Ruční testy** – prověření výsledků automatických testů, identifikace perspektivních nedostatků a skulin systémů, prověření WWW aplikací a použití metod sociálního inženýrství, demonstrace možností modifikace obsahu dat aplikací apod. Detekce reakce cíle na útoky.
- **Systematizace výsledků, závěrečná zpráva** – popis a shrnutí výsledků jednotlivých testů, identifikace zranitelností a jejich nebezpečnosti, doporučení nápravných opatření.

2.1.3. Při testování webových aplikací je dodavatel povinen vyjít z metodiky OWASP (www.owasp.org - Open Web Application Security Project). OWASP zahrnuje mnoho různých služeb, především „Guide to Building Secure Web Applications and Web Services", dále OWASP TOP TEN projekt, testovací nástroje, „OWASP Web Application Penetration Checklist" a mnoho dalších.

2.1.4. Pro prezentaci výsledků bezpečnostních testů webových aplikací objednatel vyžaduje použití metriky TOP TEN (NEJ 10), aby bylo docíleno co největšího přehledu objednatele s ohledem na aktuální zranitelnosti.

2.1.5. Metrika TOP10 zranitelností je každoročně aktualizována a je veřejně dostupná na webových stránkách OWASP.

2.1.6. URL pro TOP10 v roce 2013 na webu OWASP je následující: https://www.owasp.org/index.php/Top_10_2013-Top_10

2.1.7. Obsah testů uvedených v tomto dokumentu je považován za nezbytné minimum.

2.1.8. Testy musejí být koncipovány jako opakovatelné a reprodukovatelné tak, aby zadavatel byl schopen testy a jejich výsledek opakovat.

2.1.9. Testy nesmí poškodit cílové servery, nesmí vymazat a ani modifikovat stávající data, musí být koncipovány jako nedestruktivní. Pokud budou některé úkony testu potenciálně destruktivní, pak je nutno tyto úkony před jejich použitím předběžně odsouhlasit se zadavatelem (posoudit dopad testu a provést je nejprve v izolovaném prostředí).

Čl. 3. Definice typu požadovaných služeb

3.1. První penetrační test

3.1.1. Cílem penetračního testu je odhalit co největší množství kritických zranitelností ve webové aplikaci a prostředí, na kterém aplikace běží, odhalit způsob jejich využití a případnou možnost získání privilegovaného přístupu.

3.1.2. Tento test proběhne dle metodiky uvedené v článku 2 této Technické dokumentace a prostřednictvím testovacích scénářů, definovaných v OWASP. Dodavatel může použít i další testovací scénáře, nicméně testovací scénáře uvedené v OWASP jsou povinné.

3.1.3. Test musí kromě využití automatizovaného bezpečnostního testu zahrnovat i manuální otestování a ověření kritických zranitelností, provedených technikem – členem projektového týmu, kterým uchazeč prokazoval splnění kvalifikace.

3.1.4. Test bude zahrnovat minimálně následujících úkony, které budou popsány ve výstupní zprávě:

- Seznámení se s aplikací a její architekturou, získání informací o cílovém systému, jejich identifikace a analýza, včetně verze webového serveru, použitých modulů, aplikační platformy, identifikace síťového prostředí aj.
- Zmapování zranitelností – identifikace možných slabin a zranitelností aplikace a prostředí, ve kterém je provozována, dle metodiky OWASP, případně i podle jiné metodiky, kterou dodavatel používá
- Využití zranitelností – pokus o získání přístupu pomocí dříve identifikovaných zranitelností s cílem získat uživatelský nebo privilegovaný (administrátorský) přístup do aplikace nebo operačního systému, neoprávněné získání dat, modifikaci či poškození dat

nebo způsobení nedostupnosti testované aplikace. Prioritně bude věnována pozornost zranitelnostem s nejvyšší závažností

3.1.5. Výstupem testu bude zpráva o provedeném testu v rozsahu:

A) Manažerské shrnutí – název aplikace, v případě, že se jedná o aplikaci z projektu IOP výzvy č. 08 označení projektu, přehled hlavních zjištění a doporučení

B) Shrnutí známých informací o testované aplikaci a prostředí, s jasným oddělením toho, které informace byly předány zadavatelem před zahájením testu a které informace byly získány z testování a jsou tedy dostupné potenciálnímu útočníkovi

C) Přehledný seznam identifikovaných zranitelností, seřazený sestupně podle jejich závažnosti a jejich popis.

D) Výčet všech pokusů dodavatele o průnik a výsledek takového průniku. U dobře známých a jednoduše prokazatelných zranitelností bude uveden i postup zneužití dané zranitelnosti (např. odkazem na www stránky s postupem), případně kopie obrazovek, které demonstrují skutečné zneužití zranitelnosti.

E) Doporučený postup předcházení uvedeným zranitelnostem, pokud takový existuje, případně popis vhodných alternativních protiopatření.

3.1.6. Přílohy k výstupní zprávě o provedeném testu v elektronické podobě:

A) seznam použitých nástrojů vč. verze nástroje a příp. verze databáze testovacích vzorků

B) termíny skenů (od, do) + použitý nástroj a orientační konfigurace nastavení těchto nástrojů

C) protokoly o testech z jednotlivých nástrojů, ručních tesů a srovnání plánu a výsledku testu

3.1.7. Požadovaný rozsah výstupní zprávy o provedeném testu je 6-10 stran A4 ve formátu PDF.

3.2. Opakovaný penetrační test

3.2.1. Opakovaný test webové aplikace bude objednán zejména v případě, že byly nalezeny kritické nebo vysoké zranitelnosti a bylo prokázáno, že tyto zranitelnosti jsou zneužitelné.

3.2.2. Opakovaný test pak zadavatel objedná zejména poté, co budou zranitelnosti odstraněny dodavatelem daného řešení. Opakovaný test bude možné objednat i vícekrát po sobě, tzn. opakovaně vždy po provedení opravy zranitelností ze strany dodavatele aplikace podrobené penetračnímu testu.

3.2.3. Test bude proveden ve stejném rozsahu jako „První test webové aplikace,“ pouze s tím rozdílem, že je u dodavatele předpokládána znalost testované aplikace z předchozího testování. Zpráva o provedeném testu a její přílohy budou předloženy také ve stejném rozsahu.

3.2.4. Opakovaný test webové aplikace bude realizován vždy pouze na aplikaci, na které již byl dodavatelem proveden „První test webové aplikace.“

3.3. Individuální zranitelnosti

3.3.1. Tato služba bude objednávána v případě, kdy bude zadavatel požadovat prokázání výskytu složitější zranitelnosti na základě výstupu „Prvního testu“ nebo „Opakovaného testu,“ tzn. na základě předchozí identifikace takové zranitelnosti dodavatelem. Výstupem služby bude zpracování podrobného postupu (zpráva o individuální zranitelnosti), který povede k prokázání zranitelnosti aplikace, včetně předpřipravených skriptů nebo pomocných programů, umožňujících zranitelnost prokázat.

3.3.2. Nebude-li možné provést prokázání zranitelnosti bez provedení modifikace testované aplikace (zápis do databáze, změna či smazání souborů), omezení funkcionality aplikace nebo bude mít jiné destruktivní či omezující následky, musí být zadavatel na tuto skutečnost upozorněn se všemi možnými riziky.

3.3.3. K provedení prokázání zranitelnosti s takovým rizikem bude vyžadován písemný souhlas ze strany kontaktní osoby objednatele.

3.3.4. Dodavateli vzniká nárok na odměnu za prokázání „Individuální zranitelnosti“ dle ustanovení článku 3.3. této Technické dokumentace pouze v případě úspěšného prokázání této zranitelnosti.

3.3.5. Dodavatel služby má právo test prokázání zranitelnosti písemně odmítnout provést v případě, kdy by na provedení testu bylo potřeba výrazně více času nebo pořízení specializovaných nástrojů, kterými dodavatel nedisponuje.

Čl. 4.Seznam a popis webových aplikací

4.1. Seznam aplikací z IOP

Uvedené aplikace byly pořízeny v rámci projektů, kofinancovaných z Integrovaného operačního programu. Jejich testování bude uznatelným nákladem příslušných projektů. Na služby testů těchto aplikací a dokumenty vytvářené v souvislosti s těmito testy musí být vždy uveden rozsah informací dle ustanovení rámcové smlouvy pro penetrační testy na aplikace projektů IOP výzvy číslo 08.

Název aplikace	Platforma	Aplikační server	DB server
VIRTUOS-GALATEA	IIS+.NET	Windows server 2008 R2	MS SQL 2008
Krajská digitální spisovna	Tomcat+Java	Windows server 2008 R2	MS SQL 2008
Pracovní úložiště	Tomcat+Java – Alfresco	Windows server 2008 R2	MS SQL 2008
Datový sklad	IIS+Sharepoint 2010 SP2	Windows server 2008 R2	MS SQL 2008 R2

Webový portál	IIS+PHP – modifikovaný DRUPAL (včetně jádra)	Windows server 2008 R2	MS SQL 2008
Systém eDotace	IIS+.NET	Windows server 2008 R2	MS SQL 2008
Památková péče	IIS+.NET	Windows server 2008 R2	MS SQL 2008
Správní řízení	Proxio	Windows server 2008 x64 a Windows server 2003	MS SQL 2005
Projektové řízení	Apache+PHP	Předpokládán Windows server 2008/2012	Předpokladána aktuální Oracle RDBMS
Portál Zřizovaných organizací	IIS+PHP - Wordpress	Windows server 2008 R2	MS SQL 2008
Centrální logování	x	x	MS SQL 2008
Portál DMVS PK	IIS+.NET , ARCGIS	Windows server 2008 R2	MS SQL 2008
DTM Modul ZAKÁZKY	IIS+.NET	Windows server 2008 R2	MS SQL 2008
Vysvětlivky: x - bude doplněno vítěznému uchazeči na základě nasazení aplikace; tyto aplikace jsou v době přípravy veřejné zakázky v přípravě nebo v realizaci			

4.2. Rámcový popis aplikací z IOP a dalších aplikací, které u kterých je penetrační test objednatelem předpokládán

Dále jsou uvedené aplikace, které v současné chvíli zadavatel předpokládá, že by byly objektem penetračních testů:

4.2.1. **Virtuos-Galatea** – Jedná se o Plzeňským krajem hostovaný typ spisové služby, kterou využívají organizace v Plzeňském kraji.

4.2.2. **Krajská digitální spisovna –** Krajská digitální spisovna je nástroj pro dlouhodobé ukládání (Long Time Preservation – LTP) úředních elektronických dokumentů a spisů vzniklých jako produkt činnosti orgánů veřejné moci a jiných původců v jejich spisové službě. Je určena pro uložení dokumentů jak vzniklých přímo v elektronické podobě („digital-born“) tak do elektronické podoby převedené např. procesem autorizované konverze dokumentů. V KDS jsou ukládané dokumenty a spisy po dobu běhu skartační lhůty, tj. od jejich uzavření do jejich skartace nebo předání do Národního digitálního archivu. Řešení poskytuje původcům dokumentů jejich garantované uložení. Dokumenty jsou brány obecně jako neveřejné. Součástí řešení je i integrační rozhraní na elektronické systémy spisových služeb původců. Cílovou skupinou uživatelů jsou především krajský úřad, obecní a městské úřady v regionu. Ověřování uživatelů zajišťuje řešení SSO Plzeňského kraje, napojené na identitní prostor ePUSA. Řešení je dostupné z internetu.

4.2.3. **Datový sklad –** Datový sklad funguje jako centralizované úložiště pro převážnou většinu dat, které vznikají buď jako produkt procesů fungování krajského úřadu či jsou hromaděna z různých organizací ať už veřejné správy či jiných organizací statistických. Jedná se o manažerský informační systém, který umožňuje hlubší analýzy a hledání vzájemných souvislostí v datech, dále poskytuje informace pro vedení Plzeňského kraje a jeho zřizované organizace. Data v datovém skladu slouží jako informační zdroj nejen pro KÚPK, ale i pro PO a veřejnost. Funkcionalitou DS je, že lze bez problému pracovat s rozsáhlými soubory dat.

4.2.4. **Webový portál –** Webový portál Plzeňského kraje, který slouží jako webová prezentace Plzeňského kraje a Krajského úřadu Plzeňského kraje pro uveřejňování článků, konaných akcí, ale i struktury úřadu a povinných dokumentů.

4.2.5. **Systém eDotace –** Jedná se o dotační portál pro dotační programy vypisované Plzeňským krajem. V systému jsou vypisovány jednotlivé dotační tituly, žadatelé v systému podávají žádosti, v sytému jsou žádosti vyhodnoceny a do systému je pak zadáváno i vyúčtování takových dotací.

4.2.6. **Památková péče –** Jedná se o programové vybavení pro výkon státní správy v oblasti památkové péče poskytující funkčnost veškerých agend v oblasti památkové péče vykonávané Krajskými úřady a metodiku výkonu činnosti obcí 3. stupně (tedy obcí s rozšířenou působnosti) v Plzeňském kraji.

4.2.7. **Správní řízení –** Projekt "Elektronizace správních řízení a jejich příprava na základní registry" zajistí informační systém pro podrobnou procesní evidenci vybraných správních řízení vedených na Krajském úřadu Plzeňského kraje a to jak v I., tak ve II. instanci. IS obsahuje integraci pomocí webových služeb na spisovou službu, díky které uživatel obsluhuje spisovou službu z toho IS. V případě uložení pokuty IS předává data o záznamu v platebním kalendáři do ekonomického systému.

4.2.8. **Projektové řízení –** Elektronický systém na podporu projektového řízení. Systém se skládá z modulů evidence projektů, modulu na tvorbu a správu úkolů a obecného workflow modulu na modelování procesů. Aplikace je určena nejen zaměstnancům KÚPK, ale všem organizacím zřizovanými či vlastněnými krajem.

4.2.9. **Portál zřizovaných organizací –** Jedna část aplikace je rozcestník pro zřizované organizace (seznam aplikací pro danou organizaci), další pak převzatý přehled informací z projektového řízení (přehled úkolů, helpdesků), kde detaily už se řeší přímo v projektovém řízení. A poslední část je redakční systém, kdy zaměstnanci KUPK zveřejňují články pro zřizované organizace (přímo zřizované organizace nebudou vytvářet články).

4.2.10. **Centrální logování –** V této chvíli není realizováno, připravuje se veřejná zakázka, jejímž předmětem je dodávka softwarového řešení systému centrálního logování, tzv. SIEM (Security Information and Event Management), jeho implementace následná podpora. Jeho účelem je zajistit centrální zpracování logů, jejich normalizaci, korelaci, grafickou interpretaci a archivaci a to včetně logů generovaných samotným SIEM, zpětné dohledání událostí v čase

přes více parametrů současně, snadný a uživatelsky přívětivý přístup k výstupům SIEM dle uživateli přidělených práv a rolí a garantované bezpečné uložení vybraných citlivých logů s řízeným přístupem a ochranou proti podvrhu, modifikaci či smazání. U řešení se předpokládá webové uživatelské rozhraní. Řešení bude dostupné pouze z vnitřní sítě KÚPK.

4.2.11. **GeoPortál – Portál digitální mapy veřejné správy** Plzeňského kraje integruje přístup k mapovým aplikacím, službám a geodatům.

Portálové řešení tvoří vstupní bránu do všech komponent Geoportálu. Portál je provozován ve dvou režimech – zabezpečeném a nezabezpečeném. Uživatel, který vlastní přihlašovací údaje a příslušná oprávnění, má možnost využít funkcionality, které jsou dostupné až po přihlášení. Primárním uživatelem jsou úředníci KÚ, obcí s rozšířenou působností, obcí, projektanti a obecně i veřejnost. Ve „vnitřní“ části Geoporálu je řada evidenčních aplikací a samostatných komponent pro příjem a výdej dat.

4.2.12. **DTM (Digitální technická mapa) - Modul Zakázka –** Je určen pro práci, prezentaci dat, správu a jejich údržbu. Je primárně určen pro registrované partnery z řad správců inženýrských sítí a technické infrastruktury a obcí v Plzeňském kraji. Slouží ke vstupům (přijímání) a výstupům (výdejům) těchto dat formou zakázek pro partnery a geodety.

4.2.13. **Systém pro správu poruch silniční sítě –** Jedná se o webovou aplikaci dostupnou pro mobilní zařízení, jimiž jsou v regionu sbírány poruchy silniční sítě, prováděna inventura majetku a kontrolován stav povrchu silnic.

4.2.14. **E-shop pro Centrální nákup –** Jedná se o specifický e-shop pro zřizované a zakládané organizace Plzeňského kraje, ve kterém mohou přistoupit a objednat centrálně vysoutěžené komodity, pokládat dotazy a požadavky na centrální soutěžení komodit. Jedná se o specifický nákupní systém s omezeným počtem systémových vazeb.

4.2.15. **Pracovní úložiště -** Pracovní úložiště slouží k ukládání dat vybraných kategorií jednotlivými původci z řad obcí a organizací Plzeňského kraje. Data jsou ukládána v nestrukturované formě jako soubory, ke kterým je možné doplňovat popisná metadata. Pracovní úložiště musí zajistit spolehlivé uložení, zálohování a případnou aplikaci základních retenčních politik. V pracovním úložišti je možné zakládat a spravovat oddělená logická úložiště pro jednotlivé původce. Technicky je pracovní úložiště postavené nad DMS Alfresco. Ověřování uživatelů zajišťuje řešení SSO Plzeňského kraje, napojené na identitní prostor ePUSA. Řešení je dostupné z internetu.

Příloha č. 1 Rámcové smlouvy – Penetrační testy aplikací TCPK

Metodika přístupu poskytovatele

7 Popis nabízené metodiky

- Cíl penetračních testů

Nabízené penetrační testy budou spočívat v skenování zranitelností pomocí automatizovaných nástrojů (**automatické testy**) a v následném ručním prověřování nalezených zranitelností (**ruční testy**), jejichž cílem bude zjištění aktuálního stavu ochrany informačních aktiv proti narušení jejich důvěrnosti, integrity a dostupnosti.

- Popis penetračních testů

V průběhu provádění bezpečnostních testů se bude vycházet z testovacích scénářů, jejichž cílem je maximální pokrytí potencionálních zranitelností provozovaných systémů. Prováděné testy zranitelnosti a jejich testovací scénáře se budou dělit na:

Externí penetrační testy

Zde bude simulováno chování anonymního útočníka, který nemá žádné znalosti a přístup do testovaného provozního prostředí, tj. „black box“ testy. Testování bude prováděno přímo z prostředí Internetu.

Interní penetrační testy

Zde bude simulováno chování anonymního útočníka, který nemá žádné znalosti a přístup do testovaného provozního prostředí, tj. „black box“ testy. Testování bude prováděno pomocí vzdáleného přístupu v případě, že testované aplikace nebudou dostupné z Internetu (viz. Příloha č. 5 Výzvy – Návrh smlouvy o vzdáleném přístupu).

Prováděné penetrační testy se budou zaměřovat na aplikace a jejich zranitelnosti až do úrovně přístupu k operačnímu systému, t.j. nebude se jednat o penetrační testy aktivní síťové a bezpečnostní infrastruktury (např. směrovačů, firewallů apod.)

- Metodika a postup při provádění penetračních testů

Během realizace bezpečnostních testů a při následném hodnocení výsledků těchto testů se bude vycházet z následujících metodik:

- Open Web Application Security Project
- Web Application Security Consortium Threat Classification
- Open Source Security Testing Methodology Manual
- Information Systems Security Assessment Framework
- Technical Guide to Information Security Testing and Assessment

Testy budou prováděny v nedestruktivním a s výslovným přáním zdavatele také v destruktivním režimu. Před zahájením testů bude se zadavatelem domluvena hloubka a záběr (scope) konkrétních testů ve formě dokumentu „**Rules of Engagement**“. Tento dokument obsahuje směrnice a omezení, týkající se provedení bezpečnostních testů a uděluje testovacímu týmu formální pověření a dovolení k provedení činností v něm popsaných.

Dokument „**Rules of Engagement**“ bude obsahovat minimálně následující části a údaje:

- Časový plán
- Místo testování
- Účel a cíle testování
- Rozsah a hloubka testování
- Metodika testování, seznam testů
- Použité nástroje
- Domluvená pravidla a podmínky testování
- Informace, poskytnuté zákazníkem
- Notifikační proces a seznam
- Rizika a jejich pokrytí
- Podepsaný souhlas odpovědných osob

Prováděné **první penetrační testy** se budou skládat z těchto **základních fází**:

1. Sběr informací a identifikace testovaných cílů – pasivní fáze
   - Rekognoskace cílů – získání všech dostupných informací ohledně cílové aplikace

2. Základní skenování a průzkum testovaných cílů – aktivní fáze
   - Zjišťování cílů
   - Zjišťování síťových přístupů k aplikaci a jejím rozhraním, enumerace
   - Korelace informací a definování skenovacích cílů
   - Odhad možných dopadů
   - Vytvoření testovacího scénáře

3. Automatické skenování známých zranitelností systémů a aplikací – aktivní fáze
   - skenování zranitelností na úrovni služeb OS
   - skenování zranitelností na úrovni aplikací a aplikačních rozhraní
   - Testování autentizačních a autorizačních mechanizmů
   - Testování validace dat v aplikaci

4. Ruční testování využití detekovaných zranitelností - aktivní fáze
   - Vyloučení false positives automatického testování a ověření možností průniku a zneužití
   - Využití kombinovaných přístupů a eskalace privilegií
   - Využití různých vektorů (např. vybraných typů sociálního inženýrství)
   - Zjišťování lidských a automatických reakcí na průnik a pokusy o zametení stop

Opakované penetrační testy budou prováděny ve stejném rozsahu jako první penetrační testy s tím rozdílem, že se využijí poznatky z provedených prvních penetračních testů.

Prokázání individuálních zranitelností bude prováděno na základě zjištění zranitelnosti pomocí testů a objednání zadavatele. Bude provedena analýza možných dopadů a potřebných zdrojů a na základě vyhodnocení těchto informací zadavatel potvrdí její provedení.

- Použité nástroje pro penetrační testy

Během realizace penetračních testů se budou používat zejména tyto nástroje:

- Veřejně dostupné zdroje informací, zejména na Internetu
- Softwarové prostředky pro automatizované skenování testovaných cílů
- Softwarové prostředky pro testování využití detekovaných zranitelností

- Prezentace výsledků penetračních testů

Výstupním dokumentem realizovaných bezpečnostních testů je „Závěrečná zpráva“ ve formátu PDF, která bude obsahovat zejména následující části:

1. Manažerské shrnutí
   Stručný průřez průběhu testů včetně identifikace aplikace, přehledu nejzávažnějších nálezů a doporučení vedoucích k jejich odstranění.

2. Popis prostředí
   Shrnutí všech získaných informací o aplikaci prostředí dle zdrojů.

3. Popis provedených testů
   Popis postupů prováděných testů a jejich průběhu včetně použitých prostředků a nástrojů, časových údajů a srovnání očekávaných a skutečných výsledků.

4. Zjištěné skutečnosti
   Detailní popis zjištěných skutečností včetně klasifikace rizikovosti a možných dopadů na provozované aplikace

5. Doporučení
   Přehled doporučení vedoucích k odstranění nalezených zranitelností nebo jejich prevenci. Součástí výstupů budou i doporučení k prokázání výskytu **individuálních zranitelností**.

6. Závěrečné shrnutí
   Závěrečně zhodnocení provedených penetračních testů.

Jednotlivé podrobné protokoly a seznamy budou umístěny do přílohy dokumentu Výstupní zprávy.