SMLOUVA O PROVEDENÍ PENETRAČNÍCH TESTŮ

uzavřely v souladu s ustanovením § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, v platném znění (dále jen „OZ") tuto Smlouvu o poskytnutí služeb (dále jen „Smlouva").

Článek I - Identifikace smluvních stran

mezi:

Corpus Solutions a.s.
Společnost zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze, vložka B 5936
Se sídlem: Štětkova 1638/18, Nusle, 140 00 Praha 4
zastoupená Ing. Tomášem Přibylem, předsedou představenstva
e-mail: [redacted]
IČ 25764616
DIČ CZ 25764616
kontaktní osoba: Mgr. Pavel Cvešpr

(dále jen „**Poskytovatel**")

na straně jedné

a

Vodovody a kanalizace Pardubice, a.s.
Společnost zapsaná v obchodním rejstříku vedeném ...
Se sídlem: Pardubice, Zelené Předměstí, Teplého 2014, PSČ: 530 02
zastoupená Ing. Martinem Charvátem – místopředsedou představenstva
e-mail [redacted]
IČ 60108631
DIČ CZ60108631
kontaktní osoba Ing. Jaroslav Kubínek

(dále jen „**Objednatel**"),

na straně druhé.

dále také jen **Smluvní strany** nebo jednotlivě **Smluvní strana**.

Článek II - Vymezení pojmů a zkratek

Smlouva definuje pojmy a zkratky typické pro oblast penetračního testování a i další pojmy a zkratky, které mají v kontextu smlouvy specifický význam:

- CEH Certified Ethical Hacker (certifikace)
- CISA Certified Information Systems Auditor (certifikace)
- CPT Cone Penetration Test (certifikace)
- DNS Domain Name System
- ECSA Certified Security Analyst (certifikace)
- GIAC Global Information Assurance Certification (certifikace)
- GPEN GIAC Penetration Tester (certifikace)
- IDS Intrusion Detection System (systém detekce napadení)
- IP Internet Protocol
- IPS Intrusion Prevention System (systém prevence průniku)
- IT Informační technologie
- Úřad Národní úřad pro kybernetickou a informační bezpečnost
- OSCP Offensive Security Certified Professional (certifikace)
- OSWE Offensive Security Web Expert (certifikace)
- OSWP Offensive Security Wireless Professional (certifikace)
- PDF Portable Document Format (přenosný formát dokumentů)
- SCADA Supervisory Control And Data Acquisition (dispečerské řízení a sběr dat)

Článek III - Předmět smlouvy

a) Předmětem smlouvy je sjednání penetračního testování, jeho rozsah a atributy, včetně vymezení vzájemných práv a povinností mezi objednatelem a poskytovatelem.
b) Předmětem plnění je závazek poskytovatele k provedení penetračních testů pro předem určený rozsah zvolených IP adres.
c) Detailní specifikace testování je uvedena v příloze číslo 1. smlouvy a seznam IP adres s určením, co se na nich nachází (může se jednat například o aplikace, servery nebo operační systémy) je uveden v příloze číslo 2. smlouvy.
d) Objednatel konkretizuje závazek poskytovatele k dodržení nezbytných požadavků takto:

1. **Typ penetračních testů**

   Provedení „Grey-box testů", jejich součástí budou i „Black-box testy".

2. **Harmonogram penetračních testů**

   Při realizaci penetračního testu je nutné vzít v úvahu, že se jedná o produkční prostředí a je nutné postupovat s maximální opatrností.

   Testování musí probíhat ve dnech od Pondělí do Pátku.

   Testování musí probíhat v časech od 8 do 16.

   V harmonogramu budeje uveden:

   - Začátek penetračního testování
   - Seznam testů, jejich popis a časování
   - Termín předání pracovní verze Závěrečné zprávy
   - Termín do kdy budou odstraněny nálezy
   - Opakované penetrační testování nálezů

- Předání Závěrečné zprávy

3. **Rozsah penetračních testů**

   Detailní specifikace testování je uvedena v příloze číslo 1. smlouvy.

4. **Účast na penetračním testování**

   Penetrační testování bude provedeno bez účasti objednatele na penetračním testování.

5. **Vyhodnocení zjištěných skutečností**

   Poskytovatel je povinen při vyhodnocování zjištěných skutečností postupovat dle podpůrného materiálu NÚKIB PENETRAČNÍ TESTOVÁNÍ – ÚVOD DO PROBLEMATIKY.

6. **Pravidla vzájemné komunikace**
   Poskytovatel je povinen neprodleně o všech důležitých skutečnostech průběhu penetračního testování informovat objednatele.

7. **Seznam použitých testovacích nástrojů**
   Pro účely penetračního testování bude využita kombinace kombinaci komerčních, open source a interně vyvinutých.
   - Komerční skenery zranitelností a další nástroje (BurpSuite, Nessus apod.)
   - Online služby (Shodan, Censys, Google, SSL Labs a další..)
   - Volně dostupné nástroje a exploity (Hashcat/JTR, Nmap, Wireshark, AirSnort, NetStumbler, AirCrack, eaphammer a další)
   - Interně používané neveřejné a vyvinuté nástroje a exploity

   Použití automatických nástrojů tvoří maximálně 50 % z celkového objemu testů zbylá část testů je prováděna pentesterem manuálně.

Článek IV - Podmínky penetračního testu k platné legislativě

a) Přístup do systému v rámci smluveného penetračního testování nebude vnímán jako kybernetický bezpečnostní incident dle § 8 zákona o kybernetické bezpečnosti nebo porušení zabezpečení osobních údajů dle čl. 33 GDPR.
b) Poskytovatel je povinen postupovat v souladu s mezinárodně uznávanou metodikou a standardy pro provádění penetračních testů, jako je metodika OSSTMM a standardy NIST 800–115 a OWASP Top 10.
c) Poskytovatel je povinen zajistit sběr dat ve smyslu vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti.

Článek V - Vymezení náležitostí závěrečné zprávy

a) Závěrečná zpráva jako důkaz o tom, co bylo vykonáno musí především obsahovat:
   - manažerské shrnutí,
   - harmonogram testu,
   - přesné zadání testu,
   - omezení testu,
   - použitou metodologii,
   - nalezené problémy,

- detailní popis zranitelností,
- doporučení k odstranění nálezů,
- přehledové tabulky (tabulka nálezů, tabulka systémů apod.).

b) Tester vyhotoví pracovní verzi závěrečné zprávy o nálezech zranitelností, která popisuje zjištění na základě provedeného penetračního testu a dále uvádí:
- U každé zranitelnosti musí být uveden přesný postup ověření zranitelnosti včetně specifikace prostředí.
- U každé zranitelnosti klasifikuje její závažnost, místo výskytu, postup ověření zranitelnosti a jednoznačný odkaz testu v metodice, resp. ve standartu, který je součástí metodiky.
- Součástí zprávy je také doporučená strategie nápravy a priority v jakém pořadí zranitelnosti odstranit.

Článek VI - Provedení opakovaného penetračního testu

a) Objednatel na základě informací získaných z pracovní verze závěrečné zprávy provede:
- Nápravná opatření na testerem vybraný soubor kritických zranitelností a zranitelností doporučených testerem odstranit neprodleně.
- Objednatel seznámí testera se souborem zranitelností, u kterých provedl nápravná opatření a vyzve poskytovatele k provedení opakovaného penetračního testu se zaměřením výhradně na tento soubor zranitelností.
- Tester provede cílený penetrační test dle metodiky a výsledky testu doplní jako zjištění do čistopisu závěrečné zprávy.

Článek VII - Cena penetračního testu a platební podmínky

a) Cena penetračního testování je stanovena dohodou ve výši 432 000 Kč, bez DPH, zohledňující náročnost, rozsah a zvolenou metodiku testovaní.
b) Podkladem pro placení je faktura, která musí obsahovat vedle údajů, které musí obsahovat daňový doklad, též označení banky a číslo účtu, na který má být platba uhrazena.
c) Objednatel neposkytuje zálohy.
d) Poskytovatel je oprávněn fakturovat penetrační testování, a to po odsouhlasení akceptačního protokolu. Spolu s fakturou je poskytovatel povinen doručit objednateli akceptační protokol. Právo na úhradu faktury poskytovateli vzniká, bude-li penetrační testování poskytovatelem provedeno v požadovaném rozsahu a kvalitě a bude odpovídat podmínkám sjednaným touto smlouvou.
e) Poskytovatel je povinen na faktuře vyznačit číslo smlouvy a název zakázky. Objednatel je oprávněn fakturu poskytovateli vrátit, jestliže tato nemá náležitosti daňového dokladu či neobsahuje objednatelem požadované údaje. Po tuto dobu není objednatel v prodlení s úhradou faktury, nová lhůta splatnosti počíná plynout po doručení opravené faktury.
f) Poskytovatel je oprávněn fakturovat objednateli v písemné nebo elektronické podobě. Písemná faktura se doručuje na adresu objednatele a elektronická faktura se doručuje elektronicky na e-mailovou adresu: info@vakpce.cz.
g) Objednatel uhradí fakturu poskytovateli nejpozději do 21 dnů po jejím obdržení. Objednatel není v prodlení, uhradí-li fakturu do 21 dnů po jejím obdržení, avšak po termínu, který je na faktuře uveden jako den splatnosti. Za termín úhrady je považován den, kdy se částka připíše na bankovní účet poskytovatele.
h) Poskytovatel se zavazuje, že na jím vydaných daňových dokladech bude uvádět pouze čísla bankovních účtů, která jsou správcem daně zveřejněna způsobem umožňujícím dálkový přístup (§ 98 písm. d) zákona č. 235/2004 Sb., o dani z přidané hodnoty). V případě, že daňový doklad bude obsahovat jiný než takto zveřejněný účet, bude takovýto daňový doklad považován za neúplný a objednatel vyzve poskytovatele k jeho doplnění. Do okamžiku doplnění si objednatel vyhrazuje právo neuskutečnit platbu na základě tohoto daňového dokladu.
i) V případě, že kdykoli před okamžikem uskutečnění platby ze strany objednatele na základě této smlouvy bude o znalci poskytovateli daně z přidané hodnoty zveřejněna způsobem umožňujícím dálkový přístup skutečnost, že poskytovatel je nespolehlivým plátcem (§ 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty), má objednatel právo od okamžiku zveřejnění ponížit všechny platby

poskytovateli uskutečňované na základě této smlouvy o příslušnou částku DPH. Smluvní strany si sjednávají, že takto poskytovateli nevyplacené částky DPH odvede správci daně sám objednatel v souladu s ustanovením § 109a zákona č. 235/2004 Sb.

Článek VIII - Místo plnění

a) Penetrační testy se budou realizovat i vzdáleně, což povaha plnění organizačně i technicky umožňuje.

Článek IX - Doba trvání smlouvy

a) Doba plnění dle této smlouvy je sjednána na dobu určitou, a to
ode dne účinnosti této smlouvy do 31. 10. 2023

b) Tato smlouva může být před tímto termínem ukončena písemnou dohodou obou smluvních stran. Každá ze smluvních stran je také oprávněna tuto smlouvu vypovědět bez udání důvodu. Výpovědní lhůta se sjednává jednoměsíční a počíná plynout prvním dnem kalendářního měsíce následujícího po doručení písemného znění výpovědi druhé smluvní straně.

Článek X - Oprávněné osoby

Osoby oprávněné jednat jménem objednatele a poskytovatele při plnění smlouvy.

a) Osoby oprávněné za objednatele:

- Ing
- Ing
- B
-

b) Realizační tým poskytovatele:

Role	Jméno pracovníka	Certifikát
Projektový manažer		Prince 2
Penetrační tester		ECPPT; OSCP
Penetrační tester		CyberGym
Penetrační tester		CEH
Penetrační tester		CEH

Článek XI - Mlčenlivost a ochrana osobních údajů

a) Poskytovatel se uzavřením této smlouvy zavazuje zachovávat mlčenlivost o všech skutečnostech a informacích, o nichž se dozvěděl nebo dozví v souvislosti s uzavřením této smlouvy nebo s poskytováním plnění dle této smlouvy *(dále jen „neveřejné informace")*. Zejména se poskytovatel zavazuje nesdělovat neveřejné informace jakýmkoliv způsobem třetím osobám. Dodavatel se zavazuje zachovávat mlčenlivost o všech skutečnostech, o nichž se dozví v souvislosti poskytováním služby sjednané v této smlouvě. Povinnost poskytovatele zachovávat mlčenlivost dle věty první trvá i po skončení platnosti této smlouvy. Poskytovatel se zavazuje zajistit, aby veškeré osoby, jež se

budou podílet na poskytování služby dle této smlouvy, byly zavázány mlčenlivostí. Porušení této povinnosti mlčenlivosti je možné pouze v případech, kdy to poskytovateli ukládá zákon.

b) Poskytovatel se zavazuje, že pokud v souvislosti s realizací této smlouvy při plnění svých povinností přijde do styku s osobními/citlivými údaji ve smyslu zákona č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů, učiní veškerá opatření, aby nedošlo k neoprávněnému nebo nahodilému přístupu k těmto údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož aby i jinak nebyl porušen zákon o zpracování osobních údajů a Nařízení EU 2016/679 (GDPR).

Článek XII - Rizika spojená s průběhem penetračního testování

a) Poskytovatel je povinen v maximální možné míře eliminovat rizika spojená s průběhem penetračního testování. Jedná se především o následující oblasti:

- při provádění automatizovaných testů může dojít k odmítnutí služby (denial of service) nebo k omezení provozu,
- pád systému,
- zahlcení sítě,
- spuštění tiskáren,
- při testování autentizace může dojít k zablokování účtů,
- získání přístupu do systému a k získání citlivých dat,
- získání přístupu jako reálný uživatel nebo administrátor,
- nestandardní chování aplikace,
- nechtěná aktivita (např. e-maily zákazníkům),
- průnik do cizích systémů (dodavatelé, soukromé, VPN, ...)
- aktivace bezpečnostních mechanizmů aplikace/firewallu (může dojít k zaslání oznámení administrátorovi),
- zaplnění logovacího systému,
- poškození/zahlcení prvku nacházejícím se mezi útočícím a testovaným systémem,
- ztráta nebo znehodnocení dat,
- tvorba fiktivních registrací,
- shromažďování osobních údajů a jejich zpracovávání pro potřeby řádného provedení penetračního testování,
- při nedostatečné komunikaci může v organizaci nastat panika.

b) Poskytovatel není odpovědný za škody vzniklé v průběhu penetračního testování, pokud byl objednatel včas seznámen s riziky a byl před jejich možným vznikem varován. To neplatí, pokud tyto škody byly způsobeny úmyslným jednáním poskytovatele nebo z jeho hrubé nedbalosti.

Článek XIII - Náhrada újmy

a) Objednatel je odpovědný za škody způsobené poskytovateli jakýmkoliv porušením smluvní povinnosti, poskytovatel zase za veškerou újmu vzniklou v důsledku vadného plnění nebo porušením jiné právní povinnosti.

b) Objednal požaduje, aby měl poskytovatel po dobu účinnosti smlouvy sjednané pojištění odpovědnosti za škodu způsobenou vlastní činností v souvislosti s poskytováním penetračních testů s maximální možnou výši pojistného plnění 500 000 Kč, bez DPH.

Článek XIV - Sankční ujednání

a) Je-li objednatel v prodlení se zaplacením odměny nebo její části, je poskytovatel oprávněn požadovat zaplacení úroků z prodlení ve výši 0,04 % z dlužné částky za každý den prodlení.

b) Je-li poskytovatel v prodlení s termínem dokončení penetračního testování dle čl. 3. této smlouvy, je objednatel oprávněn požadovat zaplacení úroků z prodlení ve výši 0,5 % z odměny za každý, byť i započatý den prodlení.
c) Poruší-li poskytovatel svoje povinnosti vyplývající z čl. 8 této smlouvy, je povinen zaplatit objednateli pokutu ve výši 100.000 Kč, a to za každý jednotlivý případ porušení těchto povinností.
d) Smluvní pokuty mohou být kombinovány, tzn., že uplatnění jedné smluvní pokuty nevylučuje souběžné uplatnění jakékoliv jiné smluvní pokuty. Smluvní pokuta je splatná do 21 dnů od doručení oznámení o uplatnění smluvní pokuty jednou smluvní stranou vůči druhé smluvní straně.
e) Objednatel je oprávněn jednostranně započíst smluvní pokutu proti kterékoliv pohledávce poskytovatele vůči objednateli. Pokud by nedošlo k tomuto započtení v plném rozsahu, zavazuje se poskytovatel k doplacení dlužné částky, a to do 14 kalendářních dnů ode dne převzetí písemného oznámení objednatele.
f) Smluvní strany vylučují aplikaci ustanovení § 2050 zákona č. 89/2012 Sb., občanský zákoník, a výslovně sjednávají to, že ujednání smluvní pokuty za porušení povinností dle této smlouvy nemá vliv na právo smluvních stran na náhradu škody vzniklé z porušení povinnosti, ke které se smluvní pokuta vztahuje.
g) Závazky smluvních stran uvedené v tomto článku smlouvy trvají i po splnění všech ostatních povinností dle této smlouvy a též i v případě zániku této smlouvy.

Článek XV - Odstoupení od smlouvy

a) Kterákoli ze smluvních stran je oprávněna odstoupit od této smlouvy z důvodu podstatného porušení smlouvy druhou smluvní stranou, a to zcela v souladu s ustanovením § 2002 odst. 1 zákona č. 89/2012 Sb., občanského zákoníku.
b) Nepodstatným porušením smlouvy se rozumí zejména prodlení některé ze smluvních stran se splněním některé z povinností sjednaných touto smlouvou. Kterákoli ze smluvních stran je oprávněna od smlouvy odstoupit z důvodu nepodstatného porušení smlouvy druhou smluvní stranou, pokud tato nesplní povinnost, s jejímž splněním je v prodlení, a to ani v dodatečně stanovené lhůtě, která jí k tomu byla druhou stranou poskytnuta.
c) Chce-li některá ze smluvních stran od této smlouvy odstoupit na základě ujednání z této smlouvy vyplývajících, či dle zákona, je povinna svoje odstoupení písemně oznámit druhé straně. V odstoupení musí být dále uveden důvod, pro který strana od smlouvy odstupuje. Odstoupení musí být prokazatelně doručeno druhé smluvní straně.

Článek XVI - Závěrečná ustanovení

a) Tuto smlouvu lze měnit pouze písemným oboustranně potvrzeným ujednáním výslovně nazvaným *Dodatek ke smlouvě*. Jiné zápisy, protokoly apod. se za změnu smlouvy nepovažují.
b) Práva a povinnosti vyplývající ze smlouvy nelze bez souhlasu druhé smluvní strany převádět na třetí osobu.
c) Jakékoliv spory související s touto smlouvu se smluvní strany zavazují řešit smírnou cestou. Pokud nedojde ke smírnému urovnání sporu, může kterákoliv ze smluvních stran podat žalobu u obecného soudu místně příslušného objednateli.
d) Nastanou-li u některé ze stran skutečnosti bránící řádnému plnění této smlouvy, je povinna to ihned bez zbytečného odkladu oznámit druhé straně a vyvolat jednání zástupců oprávněných k podpisu smlouvy.
e) Smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.
f) Smluvní strana, která porušila své smluvní povinnosti a v důsledku toho došlo ke zrušení smlouvy či odstoupení od smlouvy, je povinna uhradit druhé smluvní straně veškeré účelně vynaložené náklady, které jí v souvislosti s přípravou na plnění a s plněním závazku vznikly, včetně náhrady škody případně vzniklé.
g) Smluvní strany mezi sebou výslovně ujednávají, že pokud vznikne objednateli škoda, kterou je poskytovatel povinen v souladu s právními předpisy objednateli nahradit, bude škoda hrazena v penězích.
h) Smluvní strany se dohodly na vystavování smluvní agendy (smluv a dodatků) ve dvou (2) vyhotoveních, z nichž jedno (1) náleží objednateli a jedno (1) obdrží poskytovatel.

i) Obě smluvní strany prohlašují, že došlo k dohodě o celém rozsahu této smlouvy. Prohlašují shodně, že smlouva byla uzavřena svobodně a vážně, že nebyla uzavřena v tísni ani za nápadně nevýhodných podmínek pro kteroukoliv z nich.

Přílohy smlouvy:

Příloha číslo 1. - Detailní specifikace penetračního testování

V Pardubicích, dne 8.8.2023

V Praze, dne 28.7.2023

Tomáš Přibyl

Digitálně podepsal Tomáš Přibyl
Datum: 2023.08.02 00:00:20 +02'00'