Smlouva o poskytnutí služeb
VLS-SML-2023-1332-1900

uzavřená
podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník,
ve znění pozdějších předpisů, (dále jen „**občanský zákoník**“)
(dále jen „**smlouva**“)

Článek I.
Smluvní strany

Vojenské lesy a statky ČR, s.p.
Sídlo: Pod Juliskou 1621/5, 160 00 Prah 6 - Dejvice
IČ: 00000205
DIČ: CZ00000205
Zápis v OR u Městského soudu Praha, spis. zn. ALX 256
Bankovní spojení: [redacted]
Číslo účtu: [redacted]
Zastoupená: [redacted] ředitelem
Kontaktní osoba: [redacted]
ISDS: bjds93z

(dále jen „**objednatel**“)

a

ATS-TELCOM PRAHA a.s.

Se sídlem: Nad elektrárnou 1526/45, 106 00 Praha 10
Korespondenční adresa: Milíčova 14, 130 00 Prah 3
Zastoupená: [redacted] předsedou představenstva
IČO: 61860409
DIČ: CZ 61860409
Bankovní spojení: [redacted]
Číslo účtu:
Zapsaná: V Obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 2936
Kontaktní osoba: [redacted]
ISDS: rb7cxvu

(dále jen „**poskytovatel**“)

Článek II.
Účel a předmět smlouvy

1. Touto smlouvou se poskytovatel zavazuje k řádnému a včasnému poskytnutí služeb, které jsou blíže specifikovány v čl. II odst. 3. (dále jen „**služby**"). Objednatel se zavazuje k převzetí řádně a včas poskytnutých služeb a jejich výstupů a k zaplacení sjednané ceny za jejich provedení podle podmínek sjednaných v této smlouvě.

2. Účelem pořízení služby penetračního testování a testování zranitelností je ověření odolnosti podpůrných aktiv proti působení aktuálních kybernetických hrozeb, identifikace zranitelností a návrh odstranění zjištěných nedostatků. Provedení požadované služby musí odpovídat požadavkům dle Zákona o kybernetické bezpečnosti (181/2014 Sb.) a související Vyhlášky o kybernetické bezpečnosti (82/2018 Sb.) v rozsahu stanoveném touto smlouvou.

3. Předmětem plnění je provedení komplexního souboru testů penetračního testování a testování zranitelností na úrovni infrastruktury a kritických aplikací. Uvedeným testováním budou prověřeny aktuálně instalovaná a provozovaná aktiva ICT a vybrané aplikace, jejich provozní nastavení a ošetření již známých zranitelností. Výsledky testování budou sloužit k případnému zavedení nápravných nebo dodatečných bezpečnostních opatření ke zvýšení celkové úrovně zabezpečení aktiv objednatele. Zavedení nápravných nebo dodatečných bezpečnostních opatření není předmětem plnění této smlouvy. Bližší specifikace předmětu plnění je obsažena v příloze č. 1 smlouvy.

4. Poskytovatel provede testování mezinárodně uznávanou metodikou a standardy pro provádění penetračních testů, jak jsou tyto specifikovány v příloze č. 1 smlouvy.

Článek III.
Způsob, termín a místo poskytování služeb

1. Poskytovatel je povinen poskytnout služby dle časového harmonogramu, který bude po nabytí účinnosti této smlouvy dohodnut a písemně odsouhlasen oběma smluvními stranami.
2. Místem plnění je sídlo objednatele, případně další místa stanovená touto smlouvou. Poskytovatel je oprávněn poskytovat služby i vzdáleně, pokud to jejich povaha organizačně a technicky umožňuje.
3. Závěrečnou zprávu z provedeného penetračního testování (dále jen „**Závěrečná zpráva**") poskytovatel předá objednateli nejpozději do 30 dnů od ukončení posledních testů. Náležitosti Závěrečné zprávy jsou stanoveny v příloze č. 1 této smlouvy.
4. Objednatel je povinen poskytovat poskytovateli součinnost potřebnou k řádnému plnění povinností poskytovatele dle této smlouvy. Minimální rozsah součinnosti objednatele je uveden v příloze č. 1 této smlouvy. Poskytovatel není v prodlení, pokud nemůže plnit v důsledku nedostatečné součinnosti objednatele. Termíny

plnění poskytovatele se automaticky prodlužují o dobu, po kterou poskytovatel nemohl plnit z důvodu prodlení objednatele s poskytnutím součinnosti.

5. V případě nevhodných pokynů objednatele je poskytovatel povinen na nevhodnost těchto pokynů objednatele upozornit. To neplatí, nemohl-li poskytovatel nevhodnost zjistit ani při vynaložení potřebné péče. Trvá-li objednatel na poskytování služeb dle nevhodného pokynu, má poskytovatel právo požadovat, aby tak objednatel učinil v písemné formě. Poskytovatel neodpovídá za případnou újmu či škodu vzniklou v důsledku nevhodného pokynu objednatele, na jehož nevhodnost poskytovatel upozornil, a objednatel přesto trval na jeho dodržení.

6. O předání a převzetí Závěrečné zprávy bude poskytovatelem vyhotoven akceptační protokol (dále jen „**protokol**“) ve dvou (2) vyhotoveních, který bude podepsán oběma smluvními stranami, a každá ze smluvních stran obdrží po jednom (1) vyhotovení protokolu. Objednatel je povinen vyjádřit se k protokolu nejpozději do 5 pracovních dnů od jeho předložení poskytovatelem, jinak se protokol považuje za akceptovaný.

7. Pokud objednatel uplatní písemný nárok na odstranění vad Závěrečné zprávy, zavazuje se poskytovatel tyto vady odstranit bez zbytečného odkladu, nejpozději však do 10 pracovních dnů, nestanoví-li objednatel jinak.

Článek IV.
Cena a platební podmínky

1. Celková cena za služby poskytnuté dle této smlouvy činí **789.490,- Kč** bez DPH, tj. **955.289,90 Kč** s DPH, při sazbě DPH ve výši 21 %, přičemž sazba DPH bude v případě její změny stanovena v souladu s platnými právními předpisy.

2. Celková sjednaná cena poskytovaných služeb je stanovena jako cena nejvýše přípustná a nepřekročitelná a zahrnuje zejména veškeré výlohy, výdaje a náklady vzniklé poskytovateli v souvislosti s poskytováním služeb, vyhotovením a předáním výstupů dle této smlouvy.

3. Povinnou přílohou faktury poskytovatele bude objednatelem podepsaný protokol dle čl. III odst. 6. smlouvy.

4. Cena poskytnutých služeb bude uhrazena na základě faktury — daňového dokladu za poskytnuté služby. Faktura bude vystavena po řádném poskytnutí služeb.

5. Faktura (daňový doklad) vystavená poskytovatelem musí obsahovat náležitosti stanovené právními předpisy, evidenční číslo smlouvy, a dále vyčíslení ceny služeb bez DPH, DPH a cenu služeb včetně DPH.

6. Smluvní strany se dohodly na lhůtě splatnosti faktury v délce třiceti (30) kalendářních dnů ode dne doručení faktury objednateli na adresu objednatele uvedenou v záhlaví smlouvy. V případě pochybností se má za to, že dnem doručení se rozumí třetí den ode dne odeslání faktury. Cena za poskytnuté služby se považuje za uhrazenou okamžikem připsání fakturované ceny za poskytnuté služby na bankovní účet poskytovatele.

7. Objednatel je oprávněn před uplynutím lhůty splatnosti faktury vrátit bez zaplacení fakturu, která neobsahuje náležitosti stanovené touto smlouvou nebo bude-li obsahovat chybné údaje či fakturu, ke které nebude přiložen

protokol. Poskytovatel je povinen podle povahy nesprávnosti fakturu opravit nebo nově vyhotovit. V takovém případě není objednatel v prodlení se zaplacením faktury. Okamžikem doručení náležitě doplněné či opravené faktury začne běžet nová lhůta splatnosti faktury v délce třiceti (30) kalendářních dnů.

8. Objednatel nebude poskytovat poskytovateli jakékoliv zálohy na úhradu ceny poskytovaných služeb nebo jejich části.

Článek V.
Akceptace

1. Řízení o akceptaci je zahájeno dnem předání Závěrečné zprávy dle čl. III. odst. 3 této smlouvy. Akceptační procedura zahrnuje ověření, zda Závěrečná zpráva splňuje veškeré náležitosti uvedené v příloze č. 1 smlouvy a z jejího obsahu vyplývá, že služby byly poskytnuty v souladu s jejich specifikací uvedenou v příloze č. 1 smlouvy.

2. Objednatel je oprávněn Závěrečnou zprávu odmítnout akceptovat, pokud tato vykazuje podstatné vady nebo z ní vyplývá, že služby nebyly poskytnuty v rozsahu specifikovaném touto smlouvou. Odmítnutí akceptace bude uvedeno v protokolu s výrokem „**Neakceptováno**“ s uvedením konkrétních důvodů odmítnutí akceptace. Poskytovatel je v takovém případě povinen po odstranění vytknutých vad předat Závěrečnou zprávu k zahájení nové akceptační procedury.

3. Objednatel akceptuje Závěrečnou zprávu, pokud tato vykazuje nikoliv podstatné vady (dále jen „**Akceptace s výhradou**“). Poskytovatel odstraní vytknuté vady Závěrečné zprávy nejpozději do 30 kalendářních dnů od Akceptace s výhradou. Tyto skutečnosti budou zaznamenány v protokolu vyhotoveném při Akceptaci s výhradou.

4. Povinnost poskytovatele provést a předat objednateli plnění dle této smlouvy se považuje za splněnou ke dni, ke kterému objednatel vystavil akceptační protokol s výrokem akceptováno či akceptováno s výhradou.

Článek VI.
Podmínky poskytování služeb

1. Objednatel bere na vědomí a souhlasí s tím, že v průběhu poskytování služeb může poskytovatel získat přístup k osobním údajům obsaženým v systémech objednatele. Takový přístup nebude považován za porušení zabezpečení osobních údajů ve smyslu Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, GDPR).

2. Poskytovatel při poskytování služeb nebude zpracovatelem osobních údajů ve smyslu GDPR. Pokud by se poskytovatel v průběhu plnění smlouvy stal zpracovatelem osobních údajů, zavazují se smluvní strany uzavřít samostatnou zpracovatelskou smlouvu.

3. Přístup poskytovatele do systémů objednatele v rámci poskytování služeb nebude hodnocen jako kybernetický bezpečnostní incident dle § 8 zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů.

4. Objednatel bere na vědomí, že služby penetračního testování poskytované poskytovatelem dle této smlouvy mohou vést k omezení či ohrožení provozu a fungování systémů objednatele a související infrastruktury. Objednatel dále bere na vědomí a přejímá na sebe rizika poskytování služeb penetračního testování uvedená v příloze č. 1 této smlouvy.

Článek VII.
Povinnost mlčenlivosti

1. Smluvní strany jsou si vědomy toho, že v rámci plnění závazků z této smlouvy:

   a) si mohou vzájemně vědomě nebo opomenutím poskytnout informace, které budou považovány za důvěrné (dále jen „**Důvěrné informace**“);

   b) mohou jejich zaměstnanci a osoby v obdobném postavení získat vědomou činností druhé smluvní strany nebo i jejím opomenutím přístup k Důvěrným informacím druhé smluvní strany.

2. Smluvní strany se zavazují, že žádná z nich nezpřístupní třetí osobě Důvěrné informace, které při plnění této smlouvy získala od druhé smluvní strany.

3. Třetími osobami podle čl. VII odst. 2 nejsou:

   a) zaměstnanci smluvních stran a osoby v obdobném postavení;

   b) orgány smluvních stran a jejich členové;

   c) ve vztahu k Důvěrným informacím objednatele subdodavatelé poskytovatele;

   d) ve vztahu k Důvěrným informacím poskytovatele externí dodavatelé objednatele, a to i potenciální;

   za předpokladu, že se podílejí na plnění této smlouvy nebo na plnění spojeným s plněním podle této smlouvy nebo je zpřístupnění Důvěrných informací potřebné pro výkon jejich funkce a Důvěrné informace jsou jim zpřístupněny výhradně za tímto účelem a zpřístupnění Důvěrných informací je v rozsahu nezbytně nutném pro naplnění jeho účelu a za stejných podmínek, jaké jsou stanoveny smluvním stranám v této smlouvě.

4. Smluvní strany se zavazují v plném rozsahu zachovávat povinnost mlčenlivosti a povinnost chránit Důvěrné informace vyplývající z této smlouvy a též z příslušných právních předpisů. Smluvní strany se v této souvislosti zavazují poučit veškeré osoby, které se na jejich straně budou podílet na plnění této smlouvy, o výše uvedených povinnostech mlčenlivosti a ochrany Důvěrných informací a dále se zavazují vhodným způsobem zajistit dodržování těchto povinností všemi osobami podílejícími se na plnění této smlouvy.

5. Veškeré Důvěrné informace zůstávají výhradním vlastnictvím předávající smluvní strany a přijímající smluvní strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní Důvěrné informace. S výjimkou rozsahu, který je nezbytný pro plnění této smlouvy, se smluvní strana zavazuje neduplikovat žádným způsobem Důvěrné informace

druhé smluvní strany, nepředat je třetí straně ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohli plnit tuto smlouvu. Obě smluvní strany se zároveň zavazují nepoužít důvěrné informace druhé smluvní strany jinak než za účelem plnění této smlouvy.

6. Důvěrnými informacemi jsou takové informace, které nejsou běžně dostupné a jedna ze smluvních stran projevila vůli, aby se na tyto informace vztahovala povinnost mlčenlivosti, nebo s ohledem na povahu těchto informací to lze oprávněně předpokládat Nedohodnou-li se smluvní strany výslovně písemnou formou jinak, jsou Důvěrnými informacemi dále implicitně také všechny informace, které jsou anebo by mohly být součástí obchodního tajemství, zejména popisy nebo části popisů technologických procesů a vzorců, technických vzorců a technického know-how, informace o provozních metodách, procedurách a pracovních postupech a všechny další informace, jejichž zveřejnění přijímající smluvní stranou by předávající smluvní straně mohlo způsobit škodu.

7. Bez ohledu na výše uvedená ustanovení nejsou Důvěrnými informacemi informace, které:

   a) se staly veřejně známými, aniž by jejich zveřejněním došlo k porušení závazků přijímající smluvní strany či právních předpisů;

   b) měla přijímající smluvní strana prokazatelně legálně k dispozici před uzavřením této smlouvy, pokud takové informace nebyly předmětem ujednání smluvních stran o ochraně informací obsaženého v jiné smlouvě;

   c) jsou výsledkem postupu, při kterém k nim přijímající smluvní strana dospěje nezávisle a je to schopna doložit svými záznamy nebo důvěrnými informacemi třetí strany;

   d) po podpisu této smlouvy poskytne přijímající smluvní straně třetí osoba, jež není omezena v takovém nakládání s informacemi;

   e) mají být zpřístupněny na základě zákona či jiného právního předpisu včetně práva EU nebo závazného rozhodnutí oprávněného orgánu veřejné moci.

8. Porušením povinnosti mlčenlivosti smluvní stranou jsou též případy, kdy tuto povinnost poruší kterákoliv z osob uvedených v čl. VII odst. 2, které daná smluvní strana poskytla Důvěrné informace druhé smluvní strany.

9. Ukončení účinnosti této smlouvy z jakéhokoliv důvodu se nedotkne ustanovení tohoto čl. VII **Chyba! Nenalezen zdroj odkazů.**a jejich účinnost přetrvá i po ukončení účinnosti této smlouvy, a to po dobu 5 let.

Článek VIII.

Smluvní sankce, odstoupení od smlouvy a výpověď smlouvy

1. V případě nedodržení termínu předání Závěrečné zprávy dle čl. III odst. 3 smlouvy ze strany poskytovatele je poskytovatel povinen uhradit objednateli smluvní pokutu ve výši 0,2 % z celkové ceny poskytovaných služeb bez DPH za každý i započatý kalendářní den prodlení.

2. Objednatel je povinen zaplatit poskytovateli za prodlení s úhradou faktury po sjednané lhůtě splatnosti zákonný úrok z prodlení v zákonné výši.

3. Smluvní pokuta a úrok z prodlení jsou splatné do čtrnácti (14) kalendářních dnů ode dne jejich uplatnění oprávněnou stranou.

4. Zaplacením smluvní pokuty a úroku z prodlení není dotčen nárok smluvních stran na náhradu škody v rozsahu stanoveném smlouvou ani povinnost poskytovatele dále řádně poskytovat služby.

5. Objednatel je oprávněn od této smlouvy odstoupit v případě, že:

   a) poskytovatel je v prodlení s předáním Závěrečné zprávy dle čl. III odst. 3 smlouvy delším než třicet (30) kalendářních dní;

   b) vůči majetku poskytovatele probíhá insolvenční řízení, v němž bylo vydáno rozhodnutí o úpadku, pokud to právní předpisy umožňují;

   c) insolvenční návrh na poskytovatele byl zamítnut proto, že majetek poskytovatele nepostačuje k úhradě nákladů insolvenčního řízení.

6. Poskytovatel je oprávněn od této smlouvy odstoupit v případě, že objednatel bude v prodlení s úhradou svých peněžitých závazků vyplývajících z této smlouvy po dobu delší než třicet (30) kalendářních dní.

7. Účinky odstoupení od smlouvy nastávají okamžikem doručení písemného projevu vůle odstoupit od této smlouvy druhé smluvní straně.

Článek IX.
Ostatní ujednání

1. Poskytovatel není odpovědný za škodu či újmu vzniklou objednateli či třetím osobám v důsledku poskytování služeb penetračního testování dle této smlouvy, zejména pak pokud tato vznikne v důsledku výskytu rizik penetračního testování uvedených v příloze č. 1 této smlouvy. To neplatí, pokud byla škoda či újma způsobena úmyslným jednáním poskytovatele nebo z jeho hrubé nedbalosti.

2. Žádná smluvní strana není bez předchozího písemného souhlasu druhé smluvní strany oprávněna postoupit práva a povinnosti z této smlouvy na třetí osobu.

3. Smluvní strany jsou povinny bez zbytečného odkladu oznámit změnu údajů v záhlaví smlouvy.

4. Poskytovatel je povinen dokumenty související s poskytováním služeb dle této smlouvy uchovávat nejméně po dobu deseti (10) let od konce účetního období, ve kterém došlo k zaplacení ceny poskytnutých služeb, popř. k poslednímu zdanitelnému plnění dle této smlouvy, a to zejména pro účely kontroly oprávněnými kontrolními orgány.

5. Poskytovatel je podle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), povinen spolupůsobit při výkonu finanční kontroly.

6. Poskytovatel bez jakýchkoliv výhrad souhlasí se zveřejněním své identifikace a všech dalších údajů uvedených v této smlouvě včetně ceny poskytovaných služeb.

Článek X.
Závěrečná ustanovení

1. Kontaktní osoby smluvních stran uvedené v čl. I. této jsou oprávněny k poskytování součinnosti dle této smlouvy.
2. Smlouva nabývá platnosti dnem jejího podpisu oprávněnými zástupci obou Smluvních stran a účinnosti dnem uveřejnění dle zák. č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv v registru smluv. Uveřejnění smlouvy zajistí objednatel.
3. Tato smlouva se uzavírá na dobu určitou, a to do doby úplného řádného poskytnutí služeb a jejich úplné úhrady. Zánikem účinnosti smlouvy nejsou dotčena ustanovení týkající se nároků z vad, povinnosti k náhradě škody, nároků z pokut a úroků z prodlení, ustanovení o ochraně Důvěrných informací, ani další ustanovení a nároky, z jejichž povahy vyplývá, že mají trvat i po zániku účinnosti Smlouvy.
4. Práva a povinnosti smluvních stran, které nejsou přímo upraveny touto smlouvou, se řídí příslušnými ustanoveními občanského zákoníku.
5. Smluvní strany se zavazují, že veškeré spory vzniklé v souvislosti s realizací smlouvy budou řešeny smírnou cestou. Nedojde-li k dohodě, budou spory řešeny před příslušnými obecnými soudy.
6. Veškerá korespondence mezi smluvními stranami, včetně jejich prohlášení, je ve vztahu k této smlouvě irelevantní, není-li ve smlouvě stanoveno jinak.
7. Tato smlouva může být změněna pouze dohodou smluvních stran v písemné formě.
8. Tato smlouva je podepsána elektronicky.
9. Každá ze smluvních stran prohlašuje, že tuto smlouvu uzavírá svobodně a vážně, že považuje obsah této smlouvy za určitý a srozumitelný a že jsou jí známy veškeré skutečnosti, jež jsou pro uzavření této smlouvy rozhodující, na důkaz čehož připojují smluvní strany k této smlouvě své podpisy.

Přílohy:

1) Příloha č.1 - Podrobná specifikace služeb

V Praze dne 13.07.2023

Za objednatele:

[redacted]

V Praze dne 11.07.2023

Za poskytovatele:

[redacted]

Příloha č. 1 – Podrobná specifikace služeb

Předmětem plnění je realizace jednorázových penetračních testů a skenů zranitelnosti kritických aplikací a IT infrastruktury objednatele. Cílem testování je odhalit případné zranitelnosti na systémech a službách, které by potenciální útočník mohl zneužít za účelem jejich navazujícího odstranění a zvýšení bezpečnosti systémů i celého prostředí.
Penetrační testování webových aplikací bude zaměřeno na relevantní podmnožinu zranitelností popsaných v dokumentu OWASP Top 10.

Přehled aktivit, které testovací tým bude provádět v rámci projektu na základě zadání:

Externí skeny zranitelností
Testy budou provedeny vzdálenou, neautentizovanou formou. Jejich účelem musí být identifikace existence případných zranitelností a konfiguračních nedostatků v relevantních subsystémech provozovaných objednatelem.

Interní skeny zranitelností
Testy budou provedeny vzdálenou autentizovanou formou, resp. autentizovaným způsobem a tam, kde nelze provést tento test, tak budou provedeny testy s pomocí neautentizované formy skenů:

- síťová infrastruktura.
- serverová infrastruktura.
- uživatelské stanice (vybraný vzorek)
- aplikace (ne webové)
    - ekonomický a výrobní systém
    - mzdový a personální systém

Penetrační testy webových aplikací

- Elektronická spisová služba
- Mzdový a personální systém
- Elektronický poštovní systém
- Systém pro podporu nákupu
- Systém pro správu majetku
- Systém pro vzdělávání zaměstnanců

Penetrační testy budou realizovány formou grey box/partial knowledge testu. Budou realizovány dle harmonogramu dohodnutého smluvními stranami dle čl. III odst. 1 smlouvy a až po poskytnutí všech relevantních informací pro spuštění testování a poskytnutí nezbytné součinnosti ze strany objednatele.

Penetrační testy budou realizovány z předem dohodnutých veřejných IP adres, nebo prostřednictvím VPN připojení.
V případě interního vulnerability skenu a penetračního testování může být využito fyzické návštěvy týmu poskytovatele v prostorách jednoho z datacenter, kde jsou aplikace a infrastruktura umístěny.

Součástí testů bude i bezpečnostní analýza správné implementace relevantních doporučených reaktivních opatření zveřejněných NÚKIB k odstranění závažných zranitelností.

Použité metodiky

Pro testování budou využity metodiky, které vychází z mnohaletých zkušeností bezpečnostních specialistů a kombinují různé frameworky, standardy a best practice postupy. Ty budou používány a aplikovány dle konkrétních nároků penetračního testu a řadí se mezi ně mimo jiné:

- Penetration Testing Execution Standard (PTES),
- Open Source Security Testing Methodology Manual (OSSTMM),
- NIST Special Publication (SP) 800-115,
- Metodiky Licensed Penetration Tester (LPT),
- Information Systems Security Assesment Framework (ISSAF),
- Metodiky a standardy organizace Open Web Application Security Project (OWASP):
    - Web Security Testing Guide (WSTG),
    - Mobile Security Testing Guide (MSTG),
    - Application Security Verification Standard (ASVS),
    - OWASP Top 10.

Pro potřeby evaluace charakteristiky a závažnosti zranitelnosti:

- Common Vulnerability Scoring System (CVSS) v3.1.

Při testování jsou využity pro hledání a testování na přítomnost zranitelností jak manuální postupy zmíněné v předchozích metodikách, tak pomocné a automatické nástroje pro specifické prostředí, účel, či služby. Jako příklad lze uvést aplikaci BurpSuite Pro, Tenable Nessus Professional, NMAP, SQLMap, Gobuster, Metasploit Framework a jiné.

Vymezení rozsahu dodávky

Testy a skenování zranitelností budou provedeny pro následující IP adresy:
Konkrétní IP adresy, pro něž budou provedeny testy a skeny zranitelností budou oběma smluvními stranami dohodnuty a písemně odsouhlaseny po nabytí účinnosti této Smlouvy.

Výsledky testů budou shrnuty v Závěrečné zprávě. Tato Závěrečná zpráva bude obsahovat seznam identifikovaných zranitelností z vulnerability skenování a penetračního testu, jejich detailní popis a dokumentaci, včetně konkrétního postupu umožňujícího jejich využití a ohodnocení jejich nebezpečnosti dle CVSS v3.1 a také doporučení pro jejich odstranění. Přílohy Závěrečné zprávy pak mohou obsahovat výstupy nástrojů či jiné průkazné informace, které by svojí velikostí nebyly vhodné pro formát závěrečné zprávy.

Součástí testů nebude vyhledávání zranitelností v jiných než výše uvedených aplikacích, v síťové, cloudové ani jiné infrastruktuře, virtualizačních platformách ani dalším SW vybavení serverů, které přímo nesouvisí s provozem cílového aplikačního systému. Součástí plnění

poskytovatele rovněž nebude testování odolnosti aplikace vůči volumetrickým útokům typu DoS (DDoS), testování fyzické bezpečnosti serverů, ani testy užívající phishing, nebo jiné sociotechnické postupy. Mimo rozsah plnění je také tvorba jakékoliv jiné dokumentace než výše uvedené Závěrečné zprávy a jejích příloh.

Penetrační testy jsou svou povahou invazivní. Při jejich realizaci tak není možné garantovat absenci dopadů na dostupnost testovaného systému. V případě zjištění omezené dostupnosti cílového systému nebo určité služby v důsledku testů, uvědomí testovací tým o situaci neprodleně kontaktní osobu na straně objednatele.

Závěrečná zpráva bude vypracována a předána objednateli do 30 dnů od ukončení posledních testů a bude dle požadavku objednatele obsahovat:

- manažerské shrnutí,
- harmonogram testů,
- přesné zadání testů,
- omezení testů,
- použitou metodologii,
- nalezené problémy,
- detailní popis zranitelností,
- doporučení k odstranění nálezů,
- přehledové tabulky.

Součástí výstupů testu je prezentace výsledků buď v sídle objednatele, popř. formou online schůzky.

Požadavky na součinnost objednatele

- Objednatel se zavazuje dodat poskytovateli veškeré informace potřebné pro provedení testování v rozsahu Grey Box.
- Objednatel se zavazuje vytvořit přihlašovací účty dle požadavků pro potřeby autentizovaných skenů zranitelnosti.
- Objednatel dočasně vyřadí ochrany znemožňující interní skeny zranitelností (FW, AV atp.).
- Objednatel zajistí fyzický přístup do síťové infrastruktury interního skenování pro dvě skenovací zařízení.
- Objednatel se zavazuje zajistit, aby primární kontaktní osoba na jeho straně byla poskytovateli kontinuálně dostupná v průběhu penetračních testů pro řešení případných neočekávaných situací. Touto primární kontaktní osobou na straně objednatele je: [redacted]
- Objednatel se zavazuje zajistit, aby eskalační kontakt na jeho straně byl poskytovateli kontinuálně dostupný v průběhu testů pro řešení případných neočekávaných situací. Eskalačním kontaktem objednatele je: [redacted]

Rizika penetračního testování

Objednatel souhlasí a bere na vědomí, že v průběhu penetračního testování může poskytovatel využívat v souladu se shora uvedenými podmínkami různé útočné techniky, které mohou vykazovat znaky reálného kybernetického útoku. V důsledku užití těchto technik může dojít zejména k následujícím nestandardním jevům:

- odmítnutí služby (denial of service),
- omezení provozu,
- pád systému,
- zahlcení sítě,
- spuštění tiskáren,
- zablokování účtů,
- získání přístupu do systému a získání citlivých dat,
- získání přístupu jako reálný uživatel nebo administrátor,
- nestandardní chování aplikace,
- nechtěná aktivita,
- průnik do cizích systémů,
- aktivace bezpečnostních mechanizmů aplikace/firewallu,
- 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 atd.