SMLOUVA O DÍLO

Číslo smlouvy Objednatele: 23/2023

Smluvní strany:

OTE, a.s.
se sídlem Sokolovská 192/79, Karlín, 186 00 Praha 8
IČO: 26463318
DIČ: CZ26463318
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze oddíl B, vložka 7260
Zastoupena: [redacted]
Bankovní spojení: [redacted]
Číslo účtu: [redacted]

(dále jen "**Objednatel"** nebo „**OTE, a.s.**")

a

DCIT, a.s.
se sídlem: Praha 10 - Vršovice, Kodaňská 1441/46, PSČ 10010
IČO: 26143097
DIČ: CZ26143097
zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze, oddíl B, vložka 10075
Zastoupena: [redacted]
Bankovní spojení: [redacted]
Číslo účtu: [redacted]

(dále jen "**Zhotovitel**")

(Objednatel a Zhotovitel dále každý samostatně jako „**Smluvní strana**" a společně jako „**Smluvní strany**")

uzavřely níže uvedeného dne, měsíce a roku dle ustanovení § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**Občanský zákoník**") tuto smlouvu o dílo (dále jen „**Smlouva**"):

PREAMBULE

Vzhledem k tomu, že společnost OTE, a.s. provedla průzkum trhu za účelem zadání veřejné zakázky malého rozsahu s názvem „*Penetrační testy*" (dále jen „**Veřejná zakázka**") a nabídka Zhotovitele na Veřejnou zakázku byla v souladu se zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**") vyhodnocena jako ekonomicky nejvýhodnější, dohodly se Smluvní strany v souladu na následujícím:

I. PŘEDMĚT A ÚČEL SMLOUVY

1. Zhotovitel se zavazuje na svůj náklad provést pro Objednatele dílo spočívající ve zhotovení penetračních testů blíže specifikovaných v Příloze č. 1 Smlouvy (nabídkový dokument z 27.04. 2023, článek 3.1 - varianta bez znalosti uživatelských účtů), včetně poskytnutí souvisejících plnění specifikovaných v Příloze č. 1 Smlouvy, a to vše v rozsahu a za podmínek stanovených Smlouvou (všechna výše uvedená plnění dále jen jako „**Dílo**“).

2. Dílo je blíže specifikováno v Příloze č. 1 Smlouvy, kde jsou rovněž uvedeny další související plnění, které jsou součástí Díla a jež jsou zahrnuty v ceně Díla dle čl. V. odst. 1 Smlouvy a jež se Zhotovitel zavazuje pro Objednatele provést společně s výše uvedeným plněním. Součástí Díla jsou i plnění ve Smlouvě výslovně neuvedená, pokud je to nezbytné k řádnému provedení Díla a pro úplné zajištění předmětu a účelu Smlouvy.

3. Zhotovitel podpisem Smlouvy prohlašuje, že:

   a) je oprávněn Smlouvu uzavřít a poskytovat v ní sjednané plnění,

   b) je schopen řádně plnit závazky ve Smlouvě uvedené, a

   c) se na jeho osobu, poddodavatele, jejichž prostřednictvím hodlá Zhotovitel plnit Veřejnou zakázku, jakož i na plnění, které je Zhotovitelem nabízeno, nevztahují jakékoliv mezinárodní sankce, zejména, nikoliv však výlučně, mezinárodní sankce dle (i) zákona č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů, (ii) jiných obecně závazných právních předpisů, (iii) přímo použitelných právních předpisů Evropské unie, (iv) mezinárodních smluv, dohod, úmluv či jiných dvou či vícestranných právních jednáních závazných pro Českou republiku (dále jen „**Mezinárodní sankce**“).

   Zhotovitel je povinen neprodleně písemně oznámit Objednateli, že přestal splňovat některou z podmínek dle odst. 3 tohoto článku Smlouvy, nejpozději však do pracovního dne následujícího pod dni, kdy se dozvěděl o takové skutečnosti. Zhotovitel odpovídá za újmu způsobenou Objednateli nepravdivostí výše uvedeného prohlášení či nesplněním informační povinnosti dle předchozí věty.

4. Objednatel se zavazuje řádně a včas provedené Dílo převzít a zaplatit za něj cenu podle čl. V. odst. 1 Smlouvy.

5. Smlouva se uzavírá za účelem plnění povinností Objednatele stanovených obecně závaznými právními předpisy, zejména zákona č. 458/2000 Sb., o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon), ve znění pozdějších předpisů (dále jen „**Energetický zákon**“), jakož i právními předpisy provádějícími či jinak souvisejícími s Energetickým zákonem.

II. POŽADAVKY NA PROVEDENÍ DÍLA A SOUVISEJÍCÍ PRÁVA A POVINNOSTI

1. Zhotovitel se zavazuje provést Dílo:

   a) s potřebnými znalostmi a odbornou péčí,

   b) v souladu s veškerými právními předpisy, včetně technických či jiných norem a doporučených norem, jakož i eventuálními normativními právními akty veřejné správy či samosprávy

a veškerými rozhodnutími, povoleními, souhlasy a licencemi, které mají relevanci k Dílu a jeho provedení (dále jen „**Příslušné požadavky**“),

c) bez použití osob či věcí, na které se vztahují jakékoliv Mezinárodní sankce, a

d) dle podmínek stanovených Smlouvou.

2. Zhotovitel je při provádění Díla vázán pokyny a je povinen postupovat tak, aby na majetku Objednatele nebo třetích osob nezpůsobil jakoukoliv škodu nebo jinou újmu. Zhotovitel je povinen neprodleně písemně upozornit Objednatele na nevhodnost jeho pokynů (zejména takových pokynů, jejichž následkem může vzniknout škoda či jiná újma).

3. Objednatel je povinen poskytnout Zhotoviteli součinnost nezbytnou pro provádění Díla spočívající zejména v:

a) zajištění funkčnosti a přístupnosti testovaných aplikací a systémů po potřebnou dobu,

b) zřízení testovacích účtů a poskytnutí přihlašovacích údajů Zhotoviteli před zahájením příslušných testů, je-li předmětem Díla test se znalostí autentizačních údajů,

c) poskytnutí kontaktu na osobu technicky i organizačně kompetentní koordinovat průběh provádění Díla ze strany Objednatele,

d) zabezpečení součinnosti a informovanost třetí osoby v případě, kdy se na provozování testovaného systému Objednatele podílí taková třetí osoba.

Zhotovitel je povinen v dostatečném předstihu písemně (včetně e-mailové komunikace) informovat Objednatele o rozsahu potřebné součinnosti. V případě prodlení Objednatele s poskytnutím součinnosti se lhůty uvedené v Příloze č. 2 Smlouvy odpovídajícím způsobem posouvají o dobu prodlení s poskytnutím součinnosti ze strany Objednatele.

6. Zhotovitel je povinen strpět ze strany Objednatele nebo jím pověřeného subjektu pravidelný dohled nad dodržováním veškerých povinností stanovených platnými a účinnými právními předpisy, normami a Smlouvou.

7. Objednatel je oprávněn si kdykoli vyžádat informace o stavu Díla. Zhotovitel musí tyto informace poskytnout ve lhůtě 4 (čtyř) kalendářních dnů ode dne doručení žádosti Objednatele.

8. Po celou dobu provádění Díla bude Zhotovitel zpracovávat veškerou dokumentaci o provádění Díla dle obecně závazných právních předpisů, a to výlučně v českém jazyce, není-li ve Smlouvě výslovně stanoveno jinak.

9. Zhotovitel zajistí po celou dobu provádění Díla dodržování předpisů bezpečnosti a ochrany zdraví při práci, požární ochrany, hygienických norem a předpisů pro nakládání s odpady, popř. jiných předpisů, které se k provádění Díla vztahují.

10. Zhotoviteli se zakazuje využívat k plnění Smlouvy poddodavatele, na které se vztahují jakékoliv Mezinárodní sankce. V případě poskytování plnění dle Smlouvy prostřednictvím poddodavatelů nese Zhotovitel odpovědnost vůči Objednateli jako by Smlouvu plnil sám. Objednatel má právo odmítnout plnění poskytnuté v rozporu s ustanovením tohoto odstavce Smlouvy bez dalšího a Zhotovitel je povinen toto rozhodnutí Objednatele respektovat.

11. Zhotovitel obstará vše, co je k řádnému provedení Díla potřeba (včetně zejména veškerého materiálu, strojů, pracovních pomůcek, nástrojů, licencí, a jiných věcí, jakož i zajištění veškerých povolení a jiných rozhodnutí orgánů veřejné moci, jsou-li k provedení Díla potřeba).

12. Zhotovitel je povinen vykonávat činnosti podle Smlouvy pouze takovým způsobem, aby:

a) nepoškozovaly majetek Objednatele, jejích smluvních partnerů či třetích osob či nepoškozovaly dobré jméno Objednatele.

13. Veškerá písemná oznámení, informace a sdělení požadovaná dle Smlouvy budou v českém jazyce a budou zaslána buď poštou, nebo elektronickou poštou na adresy následujících kontaktních osob:

a) za Objednatele:

(i) ve věcech smluvních a technických: [redacted], tel. [redacted], e-mail: [redacted],

b) za Zhotovitele:

(i) ve věcech smluvních: [redacted], [redacted], e-mail: [redacted]

(ii) ve věcech technických: [redacted], [redacted], e-mail: [redacted]

Smluvní strany jsou oprávněny měnit kontaktní osoby uvedené výše v tomto odstavci Smlouvy, a to na základě písemného oznámení doručeného druhé Smluvní straně a s účinností ode dne doručení takového oznámení. Kontaktní osoby uvedené výše v tomto odstavci Smlouvy nejsou bez dalšího oprávněny činit jménem Smluvních stran právní jednání směřující ke změně, doplnění či zrušení Smlouvy.

III. TERMÍNY A MÍSTO PLNĚNÍ

1. Smlouva se uzavírá na dobu určitou, a to od podpisu Smlouvy oběma Smluvními stranami až do okamžiku splnění všech práv a povinností Smluvních stran ze Smlouvy.

2. Zhotovitel se zavazuje Dílo provádět, dokončit a předat Objednateli v termínech uvedených v Příloze č. 2 Smlouvy.

3. Místem plnění a předání Díla je sídlo Objednatele. Smluvní strany se dohodli, že Zhotovitel je oprávněn předat Objednateli veškeré doklady, zprávy, doporučení a výstupy týkající se provedení Díla v elektronické formě, a to prostřednictvím e-mailu, datové schránky či jiných běžných elektronických prostředků komunikace na dálku určených Objednatelem.

IV. PŘEDÁNÍ A PŘEVZETÍ DÍLA

1. Předání Díla proběhne podepsáním předávacího protokolu oběma Smluvními stranami (dále jen „**Předávací protokol**“). Předávací protokol bude obsahovat specifikaci Zhotovitelem skutečně provedeného plnění a jeho přílohou budou závěrečné zprávy s kompletními výsledky penetračních testů včetně souvisejících doporučení, jak jsou tyto blíže specifikovány v Příloze č. 1 Smlouvy (dále jen „**Závěrečné zprávy**“).

2. Objednatel není povinen podepsat Předávací protokol a Dílo převzít v následujících případech:

a) Dílo má jakékoliv nedodělky či vady, včetně vad drobných,

b) Zhotovitel nepředal Objednateli veškeré doklady a dokumentaci související s Dílem (zejména pokud k Předávacímu protokolu nebyly přiloženy Závěrečné zprávy), a

c) Dílo, nebo jeho část, není Zhotovitelem předáno v souladu s čl. III. Smlouvy.

3. V případě, že Objednatel odmítne Dílo převzít, Smluvní strany vyhotoví o této skutečnosti písemný záznam, kde Objednatel uvede důvody pro odmítnutí převzetí Díla ve formě seznamu výhrad a termín, ve kterém je Zhotovitel povinen vyřešit výhrady Objednatele a zajistit předání Díla. Po vyřešení výhrad Objednatele bude v Předávacím protokolu uvedeno společně se seznamem výhrad Objednatele prohlášení Objednatele o jejich vyřešení. Smluvní strany pro vyloučení pochybností uvádí, že proces specifikovaný v tomto odstavci Smlouvy se může opakovat, až do řádného a úplného předání Díla bez výhrad Objednatele.

4. Vlastnické právo a nebezpečí škody na věci ke všem součástem Díla předaným Zhotovitelem Objednateli v souvislosti s plněním Smlouvy přechází na Objednatele dnem jejich převzetí Objednatelem podpisem Předávacího protokolu oběma Smluvními stranami.

V. CENA DÍLA

1. Smluvní strany se dohodly, že za provedení Díla náleží Zhotoviteli paušální odměna v celkové výši 168 000, - Kč (slovy: stošedesátosmtisíc korun českých) bez DPH (dále jen „**Cena Díla**“).

2. Cena Díla zahrnuje veškeré náklady Zhotovitele nezbytné pro řádné a včasné poskytnutí plnění dle Smlouvy Objednateli včetně nákladů souvisejících, o kterých Zhotovitel podle svých odborných znalostí měl vědět, že jsou k řádnému a kvalitnímu plnění dle Smlouvy nezbytné (např. poplatky, vedlejší náklady, náklady na dopravu a balení, licence, pojištění, inflace, kurzovní rizika, předpokládaná rizika spojená s provedením Díla, cestovní náklady apod.).

3. Smluvní strany se dohodly, že Cena Díla nezahrnuje DPH, která bude účtována ve výši dle platných předpisů k datu zdanitelného plnění.

4. Zhotovitel není oprávněn jednostranně započítat jakoukoliv pohledávku ze Smlouvy proti jakýmkoli pohledávkám Objednatele vůči Zhotoviteli.

VI. PLATEBNÍ PODMÍNKY

1. Smluvní strany se dohodly na bezhotovostním způsobu úhrady Ceny Díla v českých korunách. Stejné způsob úhrady platí i pro další případné platby za plnění dle Smlouvy.

2. Nárok na uhrazení Ceny Díla vzniká až po podpisu Předávacího protokolu oběma Smluvními stranami v souladu s čl. IV. Smlouvy. Objednatel při splnění podmínky dle předchozí věty následně uhradí Cenu Díla na základě daňového dokladu, který Zhotovitel vystaví nejdříve ke dni následujícímu po dni, ve kterém byl Předávací protokol podepsán oběma Smluvními stranami.

3. Veškeré daňové doklady dle Smlouvy musí být vystaveny s ustanovením § 435 Občanského zákoníku a se zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „**Zákon o DPH**“). Přílohou daňového dokladu na úhradu Ceny Díla musí být kopie Předávacího protokolu.

4. Veškeré daňové doklady dle Smlouvy musí mít všechny náležitosti daňového dokladu podle Zákona o DPH, doplněné o:

   a) číslo smlouvy Objednatele, a

   b) číslo bankovního účtu Zhotovitele, které musí být shodné s číslem bankovního účtu uvedeným ve Smlouvě a zároveň musí být zveřejněno správcem daně dle Zákona o DPH nebo oznámeno písemně s podpisem osoby, která podepsala Smlouvu (resp. jinou k tomu

oprávněnou osobou), a doručeno Objednateli nejpozději s doručením daňového dokladu a zároveň musí být zveřejněno správcem daně dle Zákona o DPH.

5. Splatnost všech daňových dokladů vystavených Zhotovitelem dle Smlouvy je 21 (dvacet jedna) pracovních dní ode dne doručení bezvadného a v souladu se Smlouvou vystaveného daňového dokladu v elektronické podobě Objednateli na e-mailovou adresu: [redacted]. Údaj o splatnosti uvedený Zhotovitelem na daňovém dokladu není pro splatnost rozhodující. Objednatel není v prodlení se zaplacením peněžité částky vyplývající z příslušného daňového dokladu, pokud nejpozději v poslední den splatnosti zadal příkaz svému peněžnímu ústavu (bance) k její úhradě.

6. Objednatel je oprávněn vrátit Zhotoviteli daňový doklad ve lhůtě splatnosti bez provedení příkazu k úhradě, pokud daňový doklad nemá předepsané náležitosti dle příslušných právních předpisů (zejména Zákona o DPH) a tohoto článku Smlouvy nebo má jiné faktické a právní vady v obsahu, a to s uvedením důvodu vrácení. Vadou obsahu je zejména skutečnost, kdy rozsah, předmět, výše ceny zdanitelného plnění nebo termíny opravňující fakturovat neodpovídají ustanovením ve Smlouvě uzavřené mezi Objednatelem a Zhotovitelem.

7. Zhotovitel je povinen podle povahy zjištěných vad daňový doklad opravit nebo nově vyhotovit. Vrácením daňového dokladu přestává běžet původní lhůta splatnosti. Nová lhůta splatnosti běží znovu ode dne doručení opraveného nebo nově vyhotoveného daňového dokladu Objednateli.

8. Stane-li se Zhotovitel nespolehlivým plátcem na základě rozhodnutí příslušného finančního úřadu dle § 106a Zákona o DPH, je povinen neprodleně, nejpozději však do následujícího pracovního dne ode dne nabytí právní moci takového rozhodnutí, o všech takových skutečnostech informovat Objednatele. Současně s písemným oznámením dle tohoto ustanovení zašle Zhotovitel Objednateli oznámení také elektronicky na e-mailovou adresu: [redacted]. Zhotovitel je zároveň povinen neprodleně shora uvedeným způsobem informovat Objednatele o tom, že bylo proti němu příslušným finančním úřadem zahájeno řízení podle § 106a zákona o DPH.

9. Je-li Zhotovitel ke dni poskytnutí zdanitelného plnění veden jako nespolehlivý plátce nebo stane-li se Zhotovitel nespolehlivým plátcem před zaplacením daňového dokladu vystaveného Zhotovitelem dle tohoto ustanovení nebo v případě jakýchkoli pochybností, je-li Zhotovitel nespolehlivým plátcem dle zákona o DPH, nebo není-li účet Zhotovitele zveřejněn správcem daně dle zákona o DPH, část finančního plnění podle daňového dokladu odpovídající dani z přidané hodnoty Objednatel uhradí přímo na účet příslušného správce daně v souladu s ustanovením § 109a zákona o DPH. O tuto část bude sníženo celkové finanční plnění podle daňového dokladu.

10. V případě, že Objednatel nezaplatí daňový doklad včas, je Zhotovitel oprávněn účtovat mu úrok z prodlení z nezaplacené částky bez DPH ve výši stanovené právními předpisy, nebylo-li ujednáno jinak ve Smlouvě.

VII. SMLUVNÍ POKUTY A ODPOVĚDNOST ZA ÚJMU

1. Objednatel je oprávněn požadovat po Zhotoviteli smluvní pokutu ve výši 0,1 % z Ceny Díla dle čl. V. odst. 1 Smlouvy za každý započatý den prodlení s řádným dokončením a předáním Díla nebo jeho částí v termínech dle čl. III. odst. 2 Smlouvy.

2. Nezaplatí-li Objednatel Cenu díla v termínu dle Smlouvy, je Zhotovitel oprávněn požadovat po Objednateli úrok z prodlení dle obecně závazných právních předpisů.

3. Smluvní pokuta je splatná na základě vystaveného daňového dokladu do 15 (patnácti) kalendářních dnů od uplatnění smluvní pokuty Objednatelem prostřednictvím písemné výzvy k úhradě smluvní pokuty doručené Zhotoviteli.

4. Objednatel je oprávněn jakékoli své peněžité splatné pohledávky ze Smlouvy, zejména nikoli však výlučně pohledávky na zaplacení smluvní pokuty, vůči Zhotoviteli jednostranně započítat proti jakýmkoli splatným i nesplatným pohledávkám Zhotovitele vůči Objednateli.

5. Zaplacením smluvní pokuty není nijak dotčeno právo Objednatele na náhradu majetkové a/nebo nemajetkové újmy včetně ušlého zisku.

6. Smluvní pokuty lze uplatňovat zároveň a navzájem se nevylučují ani nijak neovlivňují.

7. Zhotovitel je povinen k náhradě majetkové a/nebo nemajetkové újmy a k úhradě ušlého zisku Objednatele či třetích osob vzniklých v důsledku porušení povinnosti Zhotovitele. Za škodu se považuje i uložení pokuty orgánem veřejné moci, jakož i nároky třetích stran úspěšně uplatněné v souvislosti s porušením Smlouvy Zhotovitelem.

8. Použije-li Zhotovitel při provádění Díla poddodavatele či jinou třetí osobu, nahradí škodu jimi způsobenou stejně, jako by ji způsobil sám, a to bez ohledu na to, zda se taková třetí osoba zavázala provést určitou činnost samostatně.

9. Objednatel odpovídá za skutečnou škodu, kterou Zhotoviteli způsobí úmyslně nebo z hrubé nedbalosti, přičemž je Objednatel povinen takto vzniklou škodu Zhotoviteli nahradit. Objednatel neodpovídá za škodu, která vznikne, byť částečným, zaviněním Zhotovitele, ani za ušlý zisk Zhotovitele nebo nemajetkovou újmu Zhotovitele.

10. Žádná ze Smluvních stran není odpovědná za škodu vzniklou porušením povinnosti ze Smlouvy, prokáže-li, že jí ve splnění povinnosti dočasně nebo trvale zabránila mimořádná, nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na její vůli ve smyslu ustanovení § 2913 odst. 2 Občanského zákoníku. Překážka vzniklá ze škůdcových vnitřních poměrů nebo vzniklá až v době, kdy byl škůdce s plněním povinnosti ze Smlouvy v prodlení, ani překážka, kterou byl škůdce povinen překonat, ho však povinnosti k náhradě nezprostí.

11. Smluvní strany se zavazují upozornit druhou Smluvní stranu bez zbytečného odkladu na vzniklé překážky bránící řádnému plnění Smlouvy a dále se zavazují k vyvinutí maximálnímu úsilí k jejich odvrácení a překonání.

VIII. ZÁNIK SMLOUVY

1. Smlouvu lze ukončit následujícími způsoby:

   a) písemnou dohodu Smluvních stran, přičemž účinky ukončení Smlouvy nastanou k okamžiku stanovenému v takovéto dohodě. Nebude-li takovýto okamžik stanoven, pak tyto účinky nastanou ke dni podpisu dohody oběma Smluvními stranami, a

   b) písemným odstoupením Objednatele v případě podstatného porušení Smlouvy Zhotovitelem, kterým se rozumí zejména následující skutečnosti:

      (i) prodlení s řádným dokončením a předáním Díla nebo jeho částí v termínech dle čl. III. odst. 2 Smlouvy přesahuje 20 (dvacet) kalendářních dnů,

      (ii) opakovaný (druhý a další) výskyt totožné vady,

(iii) využití poddodavatele v rozporu s čl. II. odst. 10 Smlouvy,

(iv) opakovaný (druhý a další) případ nedodržení pokynu Objednatele při provádění Díla,

(v) Zhotovitel provádí Dílo v rozporu se Smlouvou a nezjedná nápravu ani v přiměřené lhůtě stanovené Objednatelem, které nebude kratší než 10 (deset) kalendářních dnů,

(vi) Zhotovitel způsobí újmu Objednateli úmyslně či z hrubé nedbalosti, a

(vii) ztráta jakéhokoli, zejména veřejnoprávního, oprávnění či jakékoli možnosti Zhotovitele poskytovat plnění za podmínek Smlouvy,

c) písemným odstoupením Objednatele z důvodů uvedených v ostatních ustanoveních Smlouvy nebo jejích přílohách,

d) písemným odstoupením Zhotovitele v případě, že Objednatel je v prodlení se zaplacením Ceny Díla, které trvá déle než 30 (třicet) pracovních dnů,

e) písemným odstoupením kterékoliv Smluvní strany v případě:

(i) pravomocného zjištění úpadku druhé Smluvní strany, a

(ii) rozhodnutí o likvidaci druhé Smluvní strany.

2. Účinky odstoupení od Smlouvy nastávají dnem doručení písemného projevu vůle odstoupit od Smlouvy druhé Smluvní straně (ex nunc).

3. V případě odstoupení od Smlouvy se Smluvní strany vypořádají tak, že Objednatel uhradí Zhotoviteli cenu plnění, které bylo ke dni účinků odstoupení Zhotovitelem dokončeno a Objednatelem převzato.

4. V případě odstoupení od Smlouvy z důvodu podstatného porušení Smlouvy Zhotovitelem je Zhotovitel povinen uhradit Objednateli:

a) náklady Objednatele spojené s dokončením Díla nad rámec sjednané Ceny Díla ve Smlouvě,

b) újmu způsobenou Objednateli prodlením s dokončením Díla v důsledku odstoupení od Smlouvy, a

c) všechny ostatní náklady, které by Objednateli nevznikly, kdyby Zhotovitel provedl Dílo dle Smlouvy.

5. Zánik Smlouvy nemá vliv na jakékoli právo kterékoli Smluvní strany vzniklé v souvislosti s porušením Smlouvy druhou Smluvní stranou před zánikem Smlouvy ani na práva a povinnosti Smluvních stran, které nabyly za jejího trvání (např. nárok na zaplacení smluvní pokuty, náhrady újmy, úroků z prodlení).

IX. OCHRANA DŮVĚRNÝCH INFORMACÍ A ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

1. Veškeré informace, které Zhotovitel v rámci plnění podle Smlouvy získá, jsou vyjma informací obecně známých považovány za důvěrné. Zhotovitel, jeho zaměstnanci i další spolupracující osoby jsou povinny o těchto informacích zachovávat mlčenlivost po celou dobu účinnosti Smlouvy, jakož i poté, co Smlouva zanikne. Zhotovitel se zavazuje, že veškeré důvěrné informace, které mu budou poskytnuty, nesdělí ani jinak nezpřístupní třetím osobám, ani je nepoužije v rozporu s jejich účelem pro své potřeby, přičemž se zavazuje zajistit, aby nedošlo k úniku takových informací. Zhotovitel zajistí plnění povinnosti dle předchozí věty i ze strany fyzických a právnických osob

spolupracujících se Zhotovitelem při plnění Smlouvy s tím, že Zhotovitel odpovídá za porušení předmětné povinnosti těmito osobami a tím případně vzniklou újmu.

2. Objednatel může Zhotovitele povinnosti mlčenlivosti písemně zprostit v případě, kdy má být část informací získaná/získaných podle Smlouvy poskytnuta dozorujícím nebo kontrolním orgánům Objednatele, popř. osobám, které mají právo takové informace požadovat.

3. Za důvěrné informace jsou považovány zejména všechny informace týkající se specifických činností a postupů, strategických plánů a záměrů, interních systémů, know-how, účetních a daňových skutečností Objednatele.

4. Povinnost mlčenlivosti o důvěrných informacích a ochrany důvěrných informací podle Smlouvy se vztahuje na Smluvní strany, na jejich zaměstnance, pomocníky i na všechny další třetí osoby, které některá ze Smluvních stran přizve podle Smlouvy nebo s předchozím písemným souhlasem druhé Smluvní strany, byť i k parciálnímu jednání, nebo které se vzájemně se sdělovanými informacemi jinak seznámí.

5. Smluvní strany jsou oprávněny sdělit důvěrné informace, které za trvání Smlouvy získaly, třetí osobě pouze s předchozím písemným souhlasem druhé Smluvní strany (tj. Smluvní strany, která důvěrnou informaci poskytla) s tím, že tento souhlas je vázán na povinnost příslušné Smluvní strany zavázat tuto třetí osobu, aby nakládala s těmito informacemi jako s důvěrnými a na souhlas této třetí osoby, že závazek přijímá, a to alespoň v rozsahu stanoveném Smlouvou; tím nejsou dotčeny povinnosti Smluvních stran stanovené právními předpisy pro nakládání s informacemi označenými těmito předpisy za důvěrné.

6. Veškeré informace, které se Zhotovitel jakýmkoliv způsobem dozví v souvislosti se Smlouvou, se považují za důvěrné, nevyplývá-li ze Smlouvy a/nebo z právního předpisu jinak. Informace, které poskytne Zhotovitel Objednateli, se považují za důvěrné, pouze pokud na jejich důvěrnost Zhotovitel Objednatele prokazatelným způsobem (např. v rámci nabídky) předem písemně upozornil a pokud zachování mlčenlivosti o takových informacích není v rozporu se (i) zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**“), zejména zásadou transparentnosti zakotvenou v § 6 ZZVZ, nebo (ii) zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů (dále jen „**Zákon o registru smluv**“).

7. Zhotovitel se zavazuje bezodkladně informovat Objednatele o skutečnostech nebo okolnostech, které by mohly zpochybnit jeho objektivnost nebo nezávislost při plnění závazků Zhotovitele dle Smlouvy.

8. Důvěrnými informacemi nejsou zejména:

   a) informace, které jsou Objednatelem uveřejněny,

   b) informace, které se staly veřejně známými, aniž by Zhotovitel porušil povinnosti dle Smlouvy,

   c) informace, které je Smluvní strana povinna sdělit/poskytnout podle právního předpisu nebo rozhodnutí soudu, správního či obdobného orgánu.

9. Smluvní strany se zavazují při zpracovávání osobních údajů postupovat v souladu s ustanoveními zákona č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů, nařízením 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 (dále jen „**GDPR**“) a příslušnými prováděcími předpisy. Objednatel zpracovává osobní údaje poskytnuté od Zhotovitele či jeho poddodavatelů na základě příslušné právní úpravy

za účelem plnění práv a povinností vyplývajících ze Smlouvy nebo vzniklých v souvislosti se Smlouvou a dále za účelem výkonu své působnosti podle zákona č. 458/2000 Sb., o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon) ve znění pozdějších předpisů, zákona č. 165/2012 Sb., o podporovaných zdrojích energie a o změně některých zákonů, v rozhodném znění, a souvisejících platných právních předpisů. Smluvní strana předávající osobní údaje ve smyslu čl. 4 odst. 1 GDPR (dále jen „**Osobní údaje**“) zajistí splnění veškerých podmínek nezbytných pro předání Osobních údajů vůči subjektům údajů v souladu s GDPR, zejména informuje subjekty údajů o skutečnosti, že došlo k předání konkrétních Osobních údajů přejímající Smluvní straně, a to za účelem plnění Smlouvy. V případě, že přejímající Smluvní stranou je Objednatel, Zhotovitel seznámí subjekty údajů rovněž i s podmínkami zpracování Osobních údajů, které jsou zveřejněny na webových stránkách Objednatele dostupných na adrese https://www.ote-cr.cz/cs/o-spolecnosti/ochrana-osobnich-udaju.

10. Závazky Smluvních stran uvedené v tomto článku Smlouvy trvají i po zániku Smlouvy.

X. ZÁVĚREČNÁ UJEDNÁNÍ

1. Smlouva nabývá platnosti dnem jejího podpisu oběma Smluvními stranami a účinnosti dnem jejího uveřejnění v registru smluv dle Zákona o registru smluv. Smluvní strany jsou si plně vědomy zákonné povinnosti Smluvních stran uveřejnit Smlouvu dle Zákona o registru smluv, včetně všech případných dodatků. Smluvní strany se dohodly, že Smlouvu zašle správci registru smluv k uveřejnění prostřednictvím registru smluv Objednatel. Zhotovitel je povinen zkontrolovat, že Smlouva včetně všech příloh a metadat byla řádně v registru smluv uveřejněna. V případě, že Zhotovitel zjistí jakékoli nepřesnosti či nedostatky, je povinen neprodleně o nich Objednatele informovat.
2. Smlouva a veškeré právní vztahy Smluvních stran na ní založené, s ní související, či z ní vyplývající se řídí právním řádem České republiky, zejména Občanským zákoníkem. Jakékoliv spory související se Smlouvou nebo z ní vyplývající se Smluvní strany zavazují řešit smírnou cestou. Pokud nedojde ke smírnému vyřešení sporu, bude tento spor rozhodován u obecného soudu místně příslušnému Objednateli. Tato změna v místní příslušnosti soudu je dohodou Smluvních stran ve smyslu § 89a zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů.
3. Smlouva může být měněna pouze písemně, a to právními jednáními Smluvní stran výslovně označenými za dodatky ke Smlouvě s podpisy osob oprávněných jednat za Smluvních strany na téže listině; změna jinou formou je vyloučena. Odstoupit od Smlouvy a vypovědět ji lze pouze písemně.
4. Smluvní strany si nepřejí, aby nad rámec výslovných ustanovení Smlouvy byla jakákoliv práva a povinnosti dovozovány z dosavadní či budoucí praxe zavedené mezi Smluvními stranami či zvyklostí zachovávaných obecně či v odvětví týkajícím se předmětu plnění Smlouvy, ledaže je ve Smlouvě výslovně sjednáno jinak. Vedle shora uvedeného si Smluvní strany potvrzují, že si nejsou vědomy žádných dosud mezi nimi zavedených obchodních zvyklostí či praxe.
5. Stane-li se některé ustanovení Smlouvy neplatným, neúčinným nebo nevymahatelným, nemá toto vliv na platnost, účinnost nebo vymahatelnost ostatních ustanovení Smlouvy, pokud ze Smlouvy nevyplývá, že toto ustanovení nelze od ostatního obsahu Smlouvy nebo příloh oddělit. Pro případ, že se některé ustanovení Smlouvy stane neplatným, neúčinným nebo nevymahatelným a jedná se o ustanovení oddělitelné od ostatního obsahu Smlouvy, Smluvní strany se zavazují bez zbytečných odkladů nahradit takové ustanovení ustanovením novým se stejným nebo obdobným účelem.

6. Jestliže některá Smluvní strana v určitém čase nebo opakovaně nebude požadovat plnění podle Smlouvy, v žádném případě to neovlivňuje její práva toto plnění vymáhat. Neuplatnění kteréhokoliv práva, oprávnění či opatření k nápravě podle Smlouvy kteroukoliv Smluvní stranou, ani odklad jejich uplatnění nebudou vykládány jako vzdání se těchto práv, oprávnění či opatření k nápravě. Jestliže jedna ze Smluvních stran promine porušení některého ustanovení Smlouvy, nebude to chápáno jako prominutí příštích porušení těchto ustanovení Smluvní stranou ani jiných porušení jiných ustanovení Smlouvy. Postupy podle tohoto ustanovení nebudou rovněž považovány za úzus nebo obchodní zvyklost.

7. Smluvní strany výslovně vylučují aplikaci následujících ustanovení Občanského zákoníku na Smlouvu: § 557, § 1726 věta druhá, § 1757 odst. 2, § 1764 až 1766, § 1793 až 1795, § 1796, § 1799 a § 1800, § 2004 a 2005 odst. 1, § 2050, § 2627. Není-li ve Smlouvě ujednáno jinak, odpověď jakékoli Smluvní strany na návrh druhé Smluvní strany (nabídku) s dodatkem, výhradou, omezením, změnou nebo odchylkou, není přijetím nabídky na ve smyslu § 1740 odst. 3 Občanského zákoníku, ani když podstatně nemění podmínky nabídky nebo Smlouvy.

8. V případě, že u Smluvní strany nastanou změny v kontaktních či platebních údajích, jednacích osobách, nebo jiné obdobné změny, případně dojde k přeměně Smluvní strany, je Smluvní strana, u níž došlo k těmto změnám, uvedené změny druhé Smluvní straně bez zbytečného odkladu písemně oznámit. Pokud tak neučiní, odpovídá druhé Smluvní straně za vzniklou škodu.

9. Smlouva je vyhotovena ve dvou (2) stejnopisech, z nichž každá smluvní strana obdrží po jednom (1) vyhotovení.

10. Smluvní strany shodně prohlašují, že si Smlouvu včetně příloh přečetly, s jejím obsahem souhlasí, a na důkaz těchto skutečností podle své svobodné a vážné vůle níže připojují oprávnění zástupci Smluvních stran své podpisy.

11. Pojmy a zkratky uvozené velkým počátečním písmenem užité v těle Smlouvy mají shodný význam i v přílohách Smlouvy, není-li v přílohách výslovně stanoveno jinak.

12. Nedílnou součástí Smlouvy jsou tyto přílohy:

    Příloha č. 1 – Nabídka ze dne 27.04. 2023
    Příloha č. 2 – Harmonogram

Za Objednatele:

[redacted]

Za Zhotovitele:

[redacted]

Příloha č. 1

DCIT

NABÍDKA

Nabídka: Penetrační testy

Zhotovitel:	**DCIT, a.s.** Kodaňská 1441/46 101 00 Praha 10 https://www.dcit.cz
Adresát:	**OTE, a.s.**
Poptávka:	25.04.2023 [redacted]
Ve věci nabídky je oprávněn jednat:	[redacted]
Datum vyhotovení:	27.04.2023
Platnost nabídky:	31.05.2023
Počet stran:	16

DCIT

Obsah

1 Úvod

Úvodem dovolte vyslovit poděkování za možnost podání nabídky našich služeb. Pevně věříme, že Vás nabídka zaujme a že společně navážeme oboustranně prospěšnou spolupráci, při které budeme moci využít našich dlouholetých zkušeností.

Přehled služeb DCIT

Technická bezpečnost

Ethical hacking

- Penetrační testy WWW (OWASP)
- Penetrační testy mobilních aplikací
- Penetrační testy – API / WS
- Penetrační testy – externí
- Penetrační testy – interní
- Penetrační testy SCADA
- Penetrační testy Wi-Fi
- Zátěžové testy – DoS

Konfigurační audit

- Hardening Microsoft Windows
- Hardening UNIX
- Hardening Microsoft SQL
- Hardening Oracle DB

Ostatní

- Code review
- Školení: bezpečnost WWW aplikací
- Školení: penetrační testy

Procesní bezpečnost

Analýzy

- Analýza rizik
- Analýza dopadů (BIA)
- Analýza shody se ZoKB
- Analýza shody s ISO 27000
- Analýza shody s GDPR

Informační bezpečnost

- Implementace ISMS
- Implementace BCM
- Bezpečnostní dokumentace

Ostatní

- GDPR poradenství
- Školení: implementace ISMS
- Školení: bezpečnost pro uživatele

Více informací o nabízených službách najdete na https://www.dcit.cz/cs/sluzby

2 Předmět nabídky

2.1 Služba – Prověření WWW aplikace

Při tomto testu je simulován útok na WWW aplikaci zákazníka typicky z vnějšího prostředí, tj. **konzultant simuluje počínání potenciálního útočníka provádějícího útok z Internetu**.

Jelikož jsou **WWW aplikace** ve většině případů **softwarová díla na zakázku**, obsahují chyby, které jsou rovněž typicky neopakovatelné a „na zakázku“:

- vesměs se jedná se o specifické a **jedinečné chyby** programátora (vlastní zaměstnanec či pracovník dodavatele), které se pochopitelně neobjeví v žádné z uznávaných databází publikovaných bezpečnostních slabin;
- obvykle proto – tyto do jisté míry jedinečné problémy – **neodhalí žádný automatizovaný nástroj pro testování zranitelností** (tzv. „vulnerability scanner“) – zejména zde vyniká přínos manuálních testů a bohaté zkušenosti a kombinační schopnosti našich specialistů.

Testování WWW aplikací je zaměřeno na celou řadu **slabin specifických pouze pro tento typ aplikací** a nutně proto používá poněkud odlišné metodiky a postupy než při „standardním“ penetračním testu.

2.1.1 Typy a průběh testů

K testování webových aplikací lze přistoupit různými způsoby na základě potřeb zákazníka, způsobu používání webových aplikací a nejpravděpodobnějších scénářů útoku.

Často se lze i při penetračních testech (přestože se původem jedná o termíny pocházející z funkčního testování) setkat s označením:

- Black-box test (bez znalosti),
- White-box test (se znalostí zdrojového kódu serverové strany),
- Grey-box test (s částečnou znalostí).

Důležité je spíše rozhodnout, zda test má být **bez znalosti** či **se znalostí** (především) **autentizačních údajů** (dále AÚ).

- Testování **bez znalosti AÚ** – Prověření je prováděno z anonymní úrovně. Tato fáze testu je zaměřena na odhalení **možnosti průniku** do aplikace (a dalších souvisejících prvků, např. do databází interní sítě) **„náhodným“ útočníkem** (tzv. „outsiderem“), který nemá představu o struktuře a obsahu aplikace.
- Testování **se znalostí AÚ** – Prověření je prováděno se znalostí autentizačních a autorizačních údajů pro přístup do aplikace. Výhodou je i znalosti struktury a funkcionalit aplikace. Testy jsou nejčastěji prováděny **z úrovně běžného uživatele**. Pro účely testu proto obvykle předpokládáme přístup k 1-2 uživatelským účtům. Cílem je prověření **možnosti překročení základních práv** přidělených běžnému uživateli, neboli možnost **zneužití aplikace „řádným“ uživatelem** (tzv. „insiderem“), který má k dispozici alespoň částečnou znalost o přístupu a použití aplikace. Kromě toho je možno (za předpokladu poskytnutí alespoň 2 testovacích účtů) prozkoumat možnosti (neoprávněného) přístupu pomocí jednoho uživatelského kontextu k datům jiného uživatele, případně i provést neoprávněně transakci (obecně aplikační akci) pod jinou identitou.

Nejčastěji se kombinuje test bez znalosti autentizačních údajů (např. prověření bezpečnosti aplikace proti náhodným či automatizovaným útokům z internetu) s testem se znalostí přihlašovacích údajů, kde se prověřuje především řízení přístupu a aplikační logika.

2.1.2 Použitá metodika testování (OWASP)

Postupy používané při testování webových aplikací opíráme o neustále aktualizovanou interní metodiku, dlouhodobě vycházející z doporučení a „de-facto" standardů **OWASP** (The Open Web Application Security Project), https://www.owasp.org.

Při testování dílčích bezpečnostních aspektů aplikace postupujeme s přihlédnutím k OWASP Web Security Testing Guide (WSTG).

V rámci prověření konkrétní webové aplikace jsou pak vždy testovány pouze oblasti, které jsou relevantní dané funkcionalitě aplikace.

2.1.3 Slabiny webových aplikací

Díky množství technologií a vývojových platforem, na kterých jsou aplikace provozovány, bylo nutno stanovit dostatečně abstraktní úroveň, kterou je třeba se při hledání možných zranitelností zabývat. Dlouhodobě se touto problematikou zabývají různé organizace, v prvé řadě mezinárodní sdružení MITRE (https://cwe.mitre.org) a v současné době stále populárnější otevřené sdružení vývojářů bezpečných webových aplikací – **OWASP** (www.owasp.org), k jehož konceptům a metodikám se dlouhodobě přikláníme. Právě OWASP již po řadu let vydává seznam nejrozšířenějších slabin webových aplikací, známý jako OWASP Top10.

Okruhy nejvýznamnějších problémů WWW aplikací se sice v průběhu let (logicky s vývojem aplikací a nových útoků na ně) mírně liší, nicméně z našeho dlouhodobějšího pozorování lze vysledovat některé „stálice" – nejnebezpečnější slabiny, tj. nejrozšířenější či s nejhorším dopadem na bezpečnost aplikací, jako je injekce kódu (např. SQL injection), Cross Site Scripting (XSS) atd.

2.1.4 Nástroje používané pro testování

Při testech webových aplikací je v prvé řadě zapotřebí kombinačních schopností a zkušenosti testera, nicméně existuje množství nástrojů, které postup testování značně usnadňují a zefektivňují.

Většina nástrojů je dostupná jako „Open Source" včetně plných zdrojových kódů, je proto na místě upozornit, že mnoho z používaných nástrojů je pro účely testování v DCIT interně dopracováno a upraveno, stejně tak využíváme vlastními silami vyvinuté, proprietární nástroje pro řešení speciálních či jednorázových testovacích úloh. K tomuto účelu jsou využívány obvyklé skriptovací (Python, Perl, Ruby) a programovací jazyky (Java, C).

Testovací nástroje (včetně vlastních) využívá v úvodní fázi testování DCIT jako referenci k prvotnímu průzkumu testovaného prostředí.

Naše přidaná hodnota však spočívá zejména v následném, **manuálním a velmi podrobném šetření** možných zranitelností a jejich kontextově závislých kombinací.

Automatové nástroje mohou poskytnout předběžnou představu o základních – potenciálních zranitelnostech. **Znalosti a zkušenost technických konzultantů** však umožňuje v daném prostředí (kontextu) využít potenciálních slabin a zkombinovat je v postup, vedoucí ke kompromitaci cílového systému. Právě tato schopnost nám umožňuje s vysokou mírou přesnosti stanovovat reálnou zranitelnost testovaných systémů a našim zákazníkům přináší přesnou informaci o možných způsobech napadení jejich technologií – doplněnou o námi navržené nejvhodnější způsoby řešení těchto bezpečnostních rizik.

Díky kombinaci automatizovaných testů a manuální práce zkušených testerů DCIT dokážeme poskytnout **detailní analýzu stavu zabezpečení testovaného systému společně s podrobným popisem (záznamem) testů** tak, aby bylo možno efektivně odstranit případné problémy.

2.2 Služba – Prověření bezpečnosti mobilních aplikací

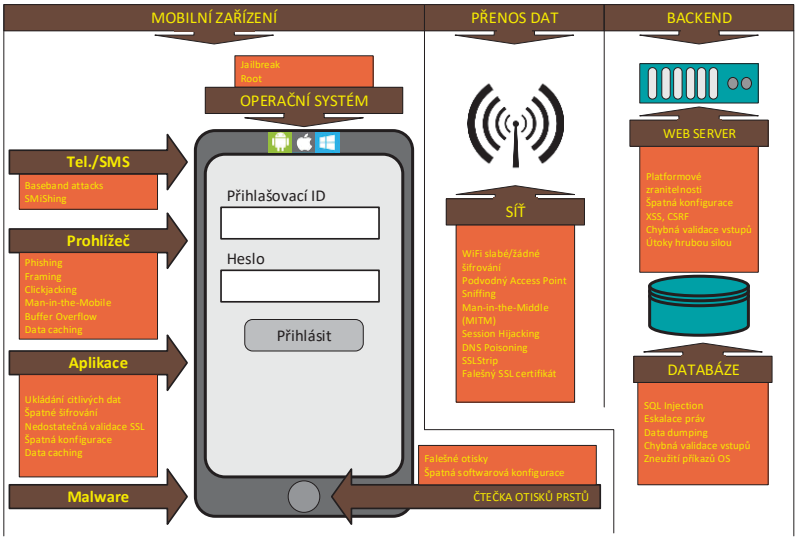
S rozšiřováním funkčnosti chytrých telefonů (smartphone) a jejich rychlého pronikání do světa internetu a seriózních aplikací typu bankovnictví (smartbanking) či nových finančních služeb, se

mobilní aplikace dostávají do také zorného úhlu profesionálních útočníků zaměřených na zisk. Současně je z principu oslabena možnost dvoukanálové autorizace transakcí či aktivit, neboť potvrzovací SMS zpráva směřuje na stejné zařízení, ze kterého byl zaslán požadavek na transakci či jinou aktivitu. Z toho důvodu je vhodné věnovat zabezpečení mobilních aplikací ještě větší pozornost než zabezpečení běžných webových aplikací.

Při tomto testu je simulován útok na mobilní zařízení a aplikaci zákazníka, tj. **tester simuluje počínání potenciálního útočníka provádějícího útok vůči serverové straně aplikace nebo samotnému mobilnímu zařízení.**

2.2.1 Anatomie útoku na mobilní aplikace

Útok může být směřován na aplikaci, na samotné mobilní zařízení (smartphone, tablet), na síť přenášející data z/do mobilního zařízení, nebo na serverovou část aplikace mnoha různými způsoby:



Jelikož jsou **mobilní aplikace** ve většině případů **softwarová díla na zakázku**, obsahují chyby, které jsou rovněž typicky neopakovatelné a „na zakázku“:

- vesměs se jedná se o specifické a **jedinečné chyby** programátora (vlastní zaměstnanec či pracovník dodavatele), které se pochopitelně neobjeví v žádné z databází publikovaných bezpečnostních slabin;
- obvykle proto - tyto do jisté míry jedinečné problémy – **neodhalí žádný automatizovaný nástroj pro testování zranitelností** (tzv. „vulnerability scanner“) – zejména zde vyniká přínos manuálních testů a bohaté zkušenosti a kombinační schopnosti našich specialistů.

Testování mobilních aplikací je zaměřeno na celou řadu **specifických slabin**, vlastních pouze tomuto typu aplikací, a nutně proto používá poněkud odlišné metodiky a postupy než při „standardním“ penetračním testu www aplikací.

2.2.2 Použitá metodika testování (OWASP)

Postupy používané při testování mobilních aplikací opíráme o neustále aktualizovanou interní metodiku, kontinuálně doplňovanou o výsledky/doporučení OWASP Mobile Security Projectu, tak aby testování pokrylo aktuální trendy vývoje zabezpečení mobilních zařízení.

2.2.3 Slabiny mobilních aplikací

Nárůst významu mobilních aplikací a tím i jejich rozšíření napříč spektrem nejrůznějších oborů a činností, kde jsou využívány při prezentaci, sběru a zpracování informací, přináší kromě nesporných výhod i řadu rizik v podobě neoprávněného přístupu a neautorizované manipulace

s daty, což může způsobit negativní dopady na chod organizací, které je provozují. Proto je čím dál důležitější pečlivě sledovat možné zranitelnosti provozovaných či právě nasazovaných aplikací a pokrýt je dříve, než může dojít k problémům.

Projekt OWASP (kromě po řadu let vydávaného seznamu nejrozšířenějších slabin webových aplikací), nově vydává OWASP Top Ten Mobile Risks.

2.2.4 Průběh testu

Test mobilní aplikace lze v zásadě rozdělit do několika fází, podle zaměření na jednotlivé části řetězce mobilní zařízení-aplikace-síť-server.

Jelikož naším cílem je provedení testu zabezpečení mobilní aplikace tak, abychom byli schopni co možná nejpřesněji určit reálnou zranitelnost aplikace vůči skutečným útokům, snažíme se co možná nejpřesněji aplikovat postupy úspěšných útočníků. Proto v testu aplikace provádíme prověření odolnosti víceméně všech komponent aplikace.

Testování probíhá v následujících fázích:

- **Testování bezpečnostního designu aplikace** – Prověření bezpečnostního designu aplikace a jeho konkrétní implementace na mobilní zařízení, zejména s ohledem na **získání, instalaci, aktivaci a autorizaci** aplikace vůči serveru s důrazem na prověření integrity aplikace v celém procesu. Dále jsou prověřovány mechanismy autentizace a autorizace klienta a způsob uložení dat (zejména citlivých) na mobilním zařízení.
- **Testování ochrany komunikace** – Prověření implementace komunikačních i aplikačních protokolů, použití a ochrana certifikátů, možnosti/nemožnosti provedení Man-In-The-Middle útoků, podvržení cookies či falešných certifikátů.
- **Testování serverové části aplikace** – Prověření řízení přístupových práv na serverové části aplikace, prověření možnosti manipulace s formátem předávaných zpráv, ověření validace vstupů na serverové straně před jejich zpracováním a ověření odolnosti serverové části proti známým útokům typu SQL injection, chyby v řízení přístupu (data mining) nebo útokům na session management.

Nabízíme dva přístupy k testování mobilních aplikací:

- **Testování bez znalosti zdrojového kódu** – konzultant provádějící test disponuje pouze omezenou znalostí samotné aplikace. Vychází především z informací běžně dostupných libovolnému uživateli aplikace. (Předpokládá se však znalost autentizačních údajů pro přístup do aplikace, certifikátů, případně představa o interní struktuře aplikace apod.)
- **Testování se znalostí zdrojového kódu aplikace** – Kromě znalostí běžného uživatele má konzultant provádějící test k dispozici zdrojový kód aplikace, který může podrobit bezpečnostní revizi. Tato úroveň testování aplikace výrazně zrychluje a tím zefektivňuje prováděné testy, neboť konzultant nemusí ztrácet čas reverzním inženýrstvím samotné aplikace, aby získal zdrojový kód.

Výsledky prověření a doporučení pro odstranění zjištěných neshod jsou součástí **závěrečné zprávy**.

2.2.5 Nástroje používané pro testování

Při testech mobilních aplikací je v prvé řadě zapotřebí kombinačních schopností a zkušeností testera, nicméně existuje množství nástrojů (i volně dostupných), které postup testování značně usnadňují a zefektivňují.

Testovací nástroje (včetně vlastních) využívá v úvodní fázi testování DCIT k prvotnímu průzkumu testované aplikace.

Automatové nástroje mohou poskytnout předběžnou představu o základních – potenciálních zranitelnostech. **Znalosti a zkušenosti testerů** však umožňují v daném prostředí (kontextu) využít potenciálních slabin a zkombinovat je v postup, vedoucí ke kompromitaci cílového systému. Právě tato schopnost nám umožňuje s vysokou mírou přesnosti stanovovat reálnou

zranitelnost testovaných systémů a našim zákazníkům přináší přesnou informaci o možných způsobech napadení jejich technologií – doplněnou o námi navržené nejvhodnější způsoby řešení nalezených bezpečnostních rizik.

Díky kombinaci automatových testů a (významného podílu) manuální práce zkušených testerů DCIT dokážeme poskytnout **detailní analýzu stavu zabezpečení testovaného systému společně s podrobným popisem (záznamem) testů** tak, aby bylo možno efektivně odstranit případné problémy.

2.3 Služba – Penetrační test API / webových služeb

Specifickým, často opomíjeným, místem, ve kterém je ohrožena bezpečnost webových aplikací, je implementace API (Application Programming Interface) rozhraní, která bývají implementována s využitím protokolu SOAP/HTTP (tzv. webové služby, webservices) nebo jako REST API. Obvykle jde o zprostředkování komunikace stroj-stroj či aplikace-aplikace. Z tohoto důvodu mu mylně nebývá věnována taková pozornost jako komunikaci uživatel-stroj/aplikace, i když dopady případných chyb mohou být fatální (únik velkého množství dat, provedení většího množství neautorizovaných transakcí).

Cílem penetračního testu API rozhraní/webových služeb je prověřit, zda je dané rozhraní bezpečné, zda pomocí něj nelze získat osobní či jiné citlivé údaje, přístup do nežádoucích oblastí nebo zda dokonce nelze cílový stroj ovládnout.

2.3.1 Varianty rozhraní

Postupy používané při testování webových služeb/API rozhraní jsou postaveny na průběžně aktualizované interní metodice, dlouhodobě vycházející z doporučení a „de-facto“ standardů OWASP – The Open Web Application Security Project.

V metodice zohledňujeme zejména doporučení sdružení OWASP určená přímo pro webové služby, uveřejněná v rámci: REST Security a XML Security Cheat Sheets.

V rámci prověření konkrétního API rozhraní/webové služby jsou pak vždy testovány pouze oblasti, které jsou relevantní pro daný typ rozhraní.

Základní typy rozhraní jsou:

- Webové služby (web services) na bázi protokolu SOAP/HTTP.
- REST API rozhraní.

SOAP (Simple Object Access Protocol) je protokolem pro výměnu zpráv založených na XML přes síť, hlavně pomocí protokolu HTTP. Základním popisem SOAP rozhraní jsou WSDL definice (opět XML), které popisují jednotlivé funkce, které dané rozhraní nabízí.

REST (Representational State Transfer) je architektura rozhraní, které definuje přístup k datům pomocí 4 základních metod (CRUD – create, retrieve, update, delete), tyto metody jsou implementovány pomocí odpovídajících HTTP metod (POST, GET, PUT, DELETE). Strukturovaná data jsou v případě REST API přenášena obvykle ve formátu JSON (může být XML, ATOM aj.).

2.3.2 Průběh testování

Testování WS/REST API není na rozdíl od jiných testů vhodné realizovat přístupem black-box (bez jakýchkoliv znalostí o předmětu testu), protože tester více času stráví otázkou „Jak to funguje?“, než „Kde je slabina?“.

Pro efektivní testování je vhodná vzorová implementace klienta, SoapUI projekt nebo podrobná dokumentace k použitým metodám a parametrům, resp. obecně popis komunikace mezi koncovými body.

Na pracnost testování má vliv počet použitých metod, parametrů, testovacích scénářů, způsob autentizace a počet uživatelských rolí, které mají být předmětem testu.

V případě webových služeb je test realizován v následujících krocích:

Typ testu	Podrobnější popis
Základní testy	Testování standardních Request(s)/Response(s) pro každou použitou metodu.
Automatizované testy	Testování API/WS pomocí specializovaných nástrojů SoapUI a BurpSuite Professional.
Identifikace zranitelností	Důkladné testy zranitelností, zejména: Fuzzing, SQLi, Malformed XML, Malicious attachment/file upload, Xpath injection, XML bomb, Authentication based attacks, External resources, Schema implementation weaknesses, Debug output, Non-encoded output.
SOAP/JSON parser	Test parseru XML/JSON. Chování aplikace při syntaktických chybách v požadavku, popřípadě při neočekávaných jinak invalidních dotazech. Obecně slabiny na úrovni zpracování vstupů (XXE apod.).
Autentizace, autorizace	Test odolnosti použité autentizační metody (Basic / SAML / OAuth / OpenID / certifikát). Možnost obcházení přístupových práv.
Parametr tampering	Manipulace s hodnotami parametrů – číselné hodnoty mimo očekávaný rozsah, vkládání neočekávaných znaků (test SQL / Xpath Injection), řetězce znaků velké délky, nekorektní formát dat oproti specifikaci.
Output encoding	Test možnosti vnutit vypsání speciálních znaků do odpovědi serveru. A to jak v samotné XML/JSON odpovědi, tak i v HTTP hlavičce. To může vést ke změně sémantiky odpovědi.
Session management	Manipulace s identifikátorem seance. Test zda je možné vnutit, podvrhnout, ukrást, nebo ovlivnit seanci. Jak se server chová na přístup k jedné seanci z různých IP.
Zátěžové testy (volitelně)	Test přítomnosti typických chyb XML/JSON parserů. Zahlcení požadavky nadměrné velikosti, příp. požadavky s vysokou komplexitou a náročností zpracování na serverové straně.

2.4 Služba – Penetrační test tlustého (těžkého) klienta

Tenkým klientem (thin client) je obvykle webový prohlížeč, který s presentační vrstvou komunikuje přes bezestavový HTTP protokol a stará se tak pouze o zobrazování dat. Na tenkém klientovi neprobíhá žádná rozhodovací logika, pokud nebereme v úvahu např. validaci dat, zadávaných do webového formuláře.

Tlustý klient (thick client) v sobě naopak obvykle obsahuje jak presentační tak i aplikační vrstvu a připojuje se přímo k databázovému nebo jinému serveru. Další typickou vlastností tlustého klienta je, že si přes síť stahuje velký objem dat, která zpracuje a výsledek pak přenese zpět na server.

Oba typy mají své výhody a nevýhody. Jedná se však typicky o **softwarová díla na zakázku**, obsahují chyby, které jsou často rovněž typicky neopakovatelné a „na zakázku“:

- vesměs se jedná se o specifické a **jedinečné chyby** programátora (vlastní zaměstnanec či pracovník dodavatele), které se pochopitelně neobjeví v žádné z uznávaných databází publikovaných bezpečnostních slabin;
- obvykle proto – tyto do jisté míry jedinečné problémy – **neodhalí žádný automatizovaný nástroj pro testování zranitelností** (tzv. „vulnerability scanner“) – zejména zde vyniká přínos manuálních testů a bohaté zkušenosti a kombinační schopnosti našich specialistů.

2.4.1 Typy a průběh testů

K testování aplikací lze přistoupit různými způsoby na základě potřeb zákazníka, způsobu používání aplikací a nejpravděpodobnějších scénářů útoku.

Často se lze i při penetračních testech (přestože se původem jedná o termíny pocházející z funkčního testování) setkat s označením:

- Black-box test (bez znalosti),

- White-box test (se znalostí),
- Grey-box test (s částečnou znalostí),

přičemž **znalostí** se obecně myslí kompletní informace o cílovém systému („full knowledge“), jako jsou zdrojové kódy, infrastruktura backendu, informace o konfiguraci apod.

Důležité je spíše rozhodnout, zda test má být **bez znalosti** či **se znalostí autentizačních údajů** (dále AÚ):

- Testování **bez znalosti AÚ** – Prověření je prováděno z anonymní úrovně. Tato fáze testu je zaměřena na odhalení **možnosti průniku** do aplikace (a dalších souvisejících prvků, např. do databází interní sítě) **„náhodným“ útočníkem** (tzv. „outsiderem“), který nemá představu o struktuře a obsahu aplikace.
- Testování **se znalostí AÚ** – Prověření je prováděno se znalostí autentizačních a autorizačních údajů pro přístup do aplikace. Výhodou je i znalosti struktury a funkcionalit aplikace. Testy jsou nejčastěji prováděny **z úrovně běžného uživatele**. Pro účely testu proto obvykle předpokládáme přístup k 1-2 uživatelským účtům. Cílem je prověření **možnosti překročení základních práv** přidělených běžnému uživateli, neboli možnost **zneužití aplikace „řádným“ uživatelem** (tzv. „insiderem“), který má k dispozici alespoň částečnou znalost o přístupu a použití aplikace. Kromě toho je možno (za předpokladu poskytnutí alespoň 2 testovacích účtů) prozkoumat možnosti (neoprávněného) přístupu pomocí jednoho uživatelského kontextu k datům jiného uživatele, případně i provést neoprávněně transakci (obecně aplikační akci) pod jinou identitou.

Nejčastěji se kombinuje test bez znalosti autentizačních údajů (např. prověření bezpečnosti aplikace proti náhodným či automatizovaným útokům) s testem se znalostí přihlašovacích údajů, kde se prověřuje především řízení přístupu a aplikační logika.

2.4.2 Použitá metodika testování (OWASP)

Ač se může zdát, že známý „de-facto“ standard **OWASP** (The Open Web Application Security Project), https://www.owasp.org se zabývá jen webovými aplikacemi, není tomu tak, v rámci svých aktivit lze nalézt doporučení i k testování tlustého klienta.

Například řada typických slabin webových aplikací je relevantních i pro tlusté klienty:

	OWASP Top Ten Most Critical Web Application Vulnerabilities	Thick Client Most Critical Application Vulnerabilities
1.	Unvalidated Input	Unvalidated Input
2.	Broken Access Control	Broken Access Control
3.	Broken Authentication and Session Management	Weak Authentication and Session Management
~~4.~~	~~Cross Site Scripting (XSS) Flaws~~	~~Not Applicable~~
5.	Buffer Overflows	Buffer Overflows
6.	Injection Flaws	Injection Flaws
7.	Improper Error Handling	Improper Error Handling
8.	Insecure Storage	Insecure Storage
9.	Denial of Service	Denial of Service
10.	Insecure Configuration Management	Insecure Configuration Management

Zdroj: Arindam Mandal: Thick Client Application Security

V rámci prověření konkrétní aplikace jsou pak vždy testovány pouze oblasti, které jsou relevantní dané funkcionalitě aplikace.

2.4.3 Typické oblasti testování tlustého klienta

Při testu tlustého klienta se zaměřujeme na především na posouzení:

- Autentizace uživatelů aplikace,
- autorizace transakcí/operací,
- možnost enumerace klientů/uživatelů,
- řízení uživatelských práv,
- komunikace aplikace (možnosti odposlechu a modifikace, MITM útoky),
- kontroly vstupů,
- způsobu ukládání (lokální vs. síťové složky) a možnosti exportu dat,
- možnosti záměrného snížení bezpečnosti ze strany klienta (např. záměrné použití velmi krátkých klíčů),
- možnosti neoprávněného získání dat z DB serveru nebo jeho napadení,
- zpracování chybových stavů aplikace,
- další testy, které vyplynou z povahy aplikace během testu.

2.4.4 Nástroje používané pro testování

Při testech tlustých klientů je v prvé řadě zapotřebí kombinačních schopností a zkušenosti testera, nicméně existuje množství nástrojů, které postup testování značně usnadňují a zefektivňují.

Většina nástrojů je dostupná jako „Open Source“ včetně plných zdrojových kódů, je proto na místě upozornit, že mnoho z používaných nástrojů je pro účely testování v DCIT interně dopracováno a upraveno, stejně tak využíváme vlastními silami vyvinuté, proprietární nástroje pro řešení speciálních či jednorázových testovacích úloh. K tomuto účelu jsou využívány obvyklé skriptovací (Python, Perl, Ruby) a programovací jazyky (Java, C).

Typově jsou potřeba především nástroje pro analýzu komunikace (různé lokální proxy). Dále pro analýzy souborového systému, v případě Win32 aplikací registry apod. Další úrovní jsou nástroje pro (de)kompilaci kódu, reverse engineering.

Testovací nástroje (včetně vlastních) využívá v úvodní fázi testování DCIT jako referenci k prvotnímu průzkumu testovaného prostředí.

Naše přidaná hodnota však spočívá zejména v následném, **manuálním a velmi podrobném šetření** možných zranitelností a jejich kontextově závislých kombinací.

Díky kombinaci automatizovaných testů a manuální práce zkušených testerů DCIT dokážeme poskytnout **detailní analýzu stavu zabezpečení testovaného systému společně s podrobným popisem (záznamem) testů** tak, aby bylo možno efektivně odstranit případné problémy.

2.5 Závěrečná zpráva

Výstupem penetračního testu je závěrečná zpráva, která obsahuje podrobnosti o průběhu testu, popis a klasifikaci nalezených zranitelností a samozřejmě doporučení ke snížení rizika.

Zpráva je rozdělena do následujících částí:

- **Manažerský souhrn** – stručný průřez průběhu testu společně s výsledky.
- **Popis testu** – popis metodiky testu a přehled všech prováděných činností.

- **Zjištěné skutečnosti** – detailní popis výsledků všech testů jednotlivých zařízení.
- **Shrnutí doporučení vyplývajících z testu** – přehledná tabulka doporučení, kterými lze odstranit nedostatky nalezené v průběhu testu.

Pro klasifikaci závažnosti zranitelnosti je standardně použita škála: Nízká (Low), Střední (Medium), Vysoká (High) a Kritická (Critical). V případě požadavku zákazníka přidáme hodnocení pomocí CVSS skóre nebo použijeme zákazníkem dodané klasifikační schéma.

	Připomínka (LOW) Takto jsou označovány nálezy s méně významným dopadem.
	Nedostatek (MEDIUM) Nálezy s nezanedbatelným dopadem, ale obtížně zneužitelné.
	**Slabina (HIGH)** Nálezy s velkým možným dopadem, vyžadující bezodkladnou opravu.
	**Velká slabina / průnik (CRITICAL)** Nálezy se zásadním dopadem, který byl demonstrován. Nutná okamžitá oprava.
	**Zlepšení / Pozitivní informace** Zlepšení oproti předchozím testům nebo dodatečná opatření zvyšující bezpečnost.

Zpráva je připravena ve formátu MS Word a PDF a zákazníkovi zaslána bezpečným způsobem.

Penetrační testy mohou být zakončeny prezentací výsledků u zákazníka – manažerská prezentace nebo technický workshop/diskuse nad závěrečnou zprávou.

3 Rozsah a cenová kalkulace

3.1 Podklady použité pro kalkulaci ceny a rozsah testu

Cenová kalkulace vychází z poptávky prezentované dokumentem „Penetrační testy OTE, a.s.pdf“ a následného upřesnění na videomeetingu 25. 4. 2023.

Penetrační testy nabízíme ve variantě bez znalosti uživatelských účtů („blackbox“; přesněji z pozice běžného uživatele internetu, protože řada informací o aplikacích je veřejně přístupná) **a ve variantě se znalostí uživatelských účtů,** která je výrazně náročnější, nicméně přináší prověření i z pohledu legitimních uživatelů a jejich možností útoku na sebe navzájem či eskalace oprávnění v rámci přidělené aplikace a jejích funkcionalit.

V případě testu bez znalosti účtů doporučujeme testovat na produkci, v případě testu se znalostí účtů doporučujeme testovat na předprodukčním prostředí a na produkci provést jen infrastrukturní test vybraných serverů (veřejně dostupných IP adres). Výjimkou je bod 1 – veřejný web společnosti, který se testuje vždy bez znalosti účtů.

3.1.1 Penetrační test WWW aplikace – veřejný web společnosti

- penetrační test webové aplikace v souladu s OWASP WSTG,
- veřejný web společnosti OTE - https://www.ote-cr.cz a https://www.ote-cr.cz/en,
- **test bez znalosti uživatelských účtů**: infratest, OWASP testy, hledání adresářů apod.
- **test se znalostí uživatelských účtů**: N/A.

3.1.2 Penetrační test WWW aplikace – portál OTE

- penetrační test webové aplikace v souladu s OWASP WSTG,
- (neveřejný) portál OTE,
- autentizace: kvalifikovaný klientský certifikát,
- počet rolí k testu: z mnoha možných rolí budou zadavatelem vybrány 2 zástupci (obvykle to jsou nejčastěji používané role nebo rizikové role z hlediska řízení přístupu, držení oprávnění apod.),
- produkční prostředí: https://portal.ote-cr.cz/otemarket/Login.jsf,
- **test bez znalosti uživatelských účtů:** infratest, OWASP testy na login page, hledání adresářů apod.
- **test se znalostí uživatelských účtů**: viz výše + testy řízení přístupu (2 subjekty).

3.1.3 Penetrační test API / WS - SOAP

- Předmětem testu bude SOAP rozhraní s počtem testovaných metod: max. 10 (celkem),
- testované rozhraní vyžaduje autentizaci + je nasazen whitelisting adres,
- vzhledem k vysokému počtu služeb a metod bude ve spolupráci se zadavatelem proveden výběr podmnožiny vhodných volání,
- **test bez znalosti uživatelských účtů:** infratest (pokud se dostaneme aspoň na whitelist),
- **test se znalostí uživatelských účtů**: viz výše + relevantní část OWASP testů, testy řízení přístupu (2 subjekty).

3.1.4 Penetrační test API / WS – AMQP

- Předmětem testu bude netypické AMQP rozhraní s počtem testovaných metod: max. 10 (celkem),
- veřejně dostupné rozhraní vyžaduje autentizaci,
- vzhledem k vysokému počtu služeb a metod bude ve spolupráci se zadavatelem proveden výběr podmnožiny vhodných volání,
- **test bez znalosti uživatelských účtů:** infratest (veřejné rozhraní),
- **test se znalostí uživatelských účtů**: není součástí nabídky z důvodu nutnosti vývoje vlastního klienta.

3.1.5 Penetrační test mobilní aplikace

- Zadání obsahuje 3 různé mobilní aplikace, vždy pro 2 platformy (Android + iOS),
- rozsah funkcionalit je velmi podobný portálu OTE,
- aplikace vyžaduje přihlášení uživatele,
- test bude proveden vzdáleně (přes internet),
- **test bez znalosti uživatelských účtů:** infratest backendových serverů, statická analýza kódu aplikace, kontrola oprávnění aplikace, obě platformy, tj. 6 aplikací.
- **test se znalostí uživatelských účtů**: infratest backendových serverů, statická analýza kódu aplikace, kontrola oprávnění aplikace + výběr 2 aplikací na Android platformě (z důvodu velké podobnosti aplikací).

3.1.6 Penetrační test tlustého klienta OTE-COM

- Produkční verze: https://www.ote-cr.cz/lm/OTE-COM-POWER-PROD-windows-x64.exe a https://www.ote-cr.cz/lm/OTE-COM-GAS-PROD-windows-x64.exe s dokumentací na https://www.ote-cr.cz/cs/dokumentace/dokumentace-elektrina/files_dokumentace/prezentace-otecom-vdt-vt.pdf,
- **test bez znalosti uživatelských účtů:** základní bezpečnostní testy, tj. autentizace, komunikace a instalace aplikace.
- **test se znalostí uživatelských účtů**: viz výše + detailní test 1 aplikace pro jednu komoditu (z důvodu podobnosti aplikací).

3.2 Potřebná součinnost

Pro úspěšné provedení nabízených služeb je třeba následující součinnost.

3.2.1 Webové aplikace, API, mobilní aplikace, thick client

- specifikace URLs testovaných prostředí,
- poskytnutí 1-2 testovacích účtů do testované aplikace pro každou z testovaných rolí, včetně autentizačních údajů a prostředků (certifikátů),
- aktivní spolupráce při výběru vhodných API endpointů a metod pro test webových služeb,
- podrobná dokumentace k API (v případě testu se znalostí účtů),
- (volitelně, ale doporučeno) zdrojové kódy mobilních aplikací,
- (volitelně, ale doporučeno) zdrojové kódy aplikací typu tlustý klient,
- (volitelně, ale doporučeno) testovací scénáře workflow, které zadavatel vnímá jako rizikové.

3.2.2 Ostatní

- závěrečná zpráva bude zpracována v češtině,
- předpokládaná realizace 2023-Q3.

3.3 Cena

Cenová a časová náročnost je uvedena v následujících tabulkách.

Položka	Trvání	Cena (bez DPH)
Penetrační testy 6 oblastí bez znalosti uživatelských účtů (varianta A)	Cca 2 týdny	168 000 Kč
Penetrační testy 6 oblastí bez znalosti + se znalostí uživatelských účtů (varianta B)	Cca 2 měsíce	[redacted]

4 Informace o DCIT, a.s.

4.1 Identifikační a kontaktní údaje

DCIT, a.s. (dále jen DCIT) je společnost působící více než 25 let v oblasti informačních technologií, která svým zákazníkům poskytuje širokou škálu komplexních služeb ve dvou hlavních oblastech, kterými jsou poradenské služby v oblasti IT a vývoj software.

jméno společnosti:	DCIT, a.s.
sídlo společnosti:	Kodaňská 1441/46, 101 00 Praha 10
statutární zástupce:	[redacted]
IČ:	26143097
DIČ:	CZ26143097
zápis v OR:	Městský soud Praha, oddíl B, vložka 10075
telefon:	[redacted]
WWW:	https://www.dcit.cz/cs

4.2 Kvalifikační předpoklady

Společnost DCIT:

- Je držitelem certifikátu NBÚ pro přístup k utajovaným informacím: https://www.dcit.cz/download/DCIT-NBU-osvedceni.pdf
- Je držitelem certifikátu managementu kvality dle normy ČSN ISO 9001: https://www.dcit.cz/download/DCIT-ISO9001-cs.pdf
- Má sjednáno pojištění odpovědnosti za škodu pro služby, které jsou předmětem jejího podnikání, s limitem plnění 20 milionů Kč. Certifikát o sjednaném pojištění: https://www.dcit.cz/download/DCIT-Pojisteni.pdf
- Výroční zprávy společnosti DCIT, a.s. jsou k dispozici na adrese: https://www.dcit.cz/cs/firma/pro-akcionare

Společnost DCIT disponuje týmem kvalitních odborníků, kteří jsou:

- Členové odborných sdružení a asociací (např. ISACA – Information Systems Audit and Control Association).
- Držitelé odborných certifikátů (např. CISA – Certified Information Systems Auditor, CRISC – Certified in Risk and Information Systems Control, CEH – Certified Ethical Hacker, OSCP – Offensive Security Certified Professional).
- Prověřeni Národním bezpečnostním úřadem pro stupeň Důvěrné.

Uvedené certifikáty a prověření jsme připraveni patřičně doložit.

1 Harmonogram projektu

Začátek penetračních testů: 14.6.2023

Konec penetračních testů: 30.6.2023

Předání závěrečné zprávy: do 7.7.2023.

Termíny jsou platné v případě poskytnutí potřebné součinnosti pro realizaci testů.