

2. Smluvní strany

- 2.1. Zhotovitel prohlašuje, že splňuje veškeré podmínky a požadavky v této smlouvě stanovené, disponuje potřebnými odbornými znalostmi a kapacitami a je oprávněn tuto smlouvu uzavřít a řádně plnit povinnosti v ní obsažené.
- 2.2. Zhotovitel je připraven plnit své povinnosti vyplývající z této smlouvy a realizovat předmět Veřejné zakázky v souladu s principy „best practice“ dle svého nejlepšího vědomí, ve prospěch Objednatele a s ohledem na úsporu jeho nákladů.

3. Předmět a účel smlouvy

- 3.1. Účelem této smlouvy je především zajištění plnění povinností Objednatele ve vztahu k dosažení potřebné úrovně kybernetické bezpečnosti informačních a komunikačních systémů a technologií, jak jsou tyto povinnosti stanoveny a nebo vyplývají z právní úpravy dané zejména zákonem č. 264/2025 Sb., o kybernetické bezpečnosti, vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti ve znění pozdějších předpisů a dle opatření, doporučení a stanovisek Národního úřadu pro kybernetickou a informační bezpečnost. Účelem této smlouvy je na základě Zhotovitelem provedeného auditu stanovit taková opatření, jejichž přijetí posílí úroveň kybernetické a informační bezpečnosti Objednatele, jenž tak bude schopen předcházet a čelit známým či předpokládaným hrozbám pro jím provozované informační a komunikační systémy a technologie a bude schopen efektivně zvládat případné následky (dopady) kybernetických incidentů. Takto definovaný účel smlouvy je také základním vodítkem a principem pro výklad všech ujednání obsažených v této smlouvě.
- 3.2. Předmětem smlouvy je zpracovat:
 - a) Audit kybernetické bezpečnosti vypracovaný v rozsahu a způsobem, který splní jak zákonné povinnosti Objednatele¹⁾, tak bude respektovat opatření, doporučení a stanoviska Národního úřadu pro kybernetickou a informační bezpečnost,
 - b) Zjištění (včetně provedení odpovídajících penetračních testů a testu zranitelnosti) aktuálního stavu kybernetické bezpečnosti digitálního prostředí Objednatele, tzn. ověření, zda realizované výstupy dílčích částí projektu jako celku, tj. ve společné synergii splňují požadavky a cíle jejich zadání – podrobněji viz Příloha č. 1,
 - c) Vyhodnocení jak realizace výše odkazovaného projektu skutečně zvýšila kybernetickou bezpečnost informačních aktiv Objednatele a konkrétní specifikace případných nedostatků aktuálního stavu kybernetické bezpečnosti Objednatele, jejich prioritizace dle závažnosti a návrh konkrétních opatření²⁾ k nápravě, která zajistí schopnost Objednatele předcházet a čelit známým či předpokládaným hrozbám pro jím provozované informační a komunikační systémy a technologie a schopnost efektivně zvládat případné následky (dopady) kybernetických incidentů.Souhrnně (tzn. v plném rozsahu všech třech výše uvedených bodů).
- 3.3. Zhotovitel je povinen plnit své povinnosti dle odst. 3.1. této smlouvy počínaje její účinností a v rozsahu a za podmínek blíže upravených v Příloze č. 1.
- 3.4. Smluvní strany se dohodly, že zjištění výchozího stavu kybernetické bezpečnosti se provede na základě dokumentace poskytnuté Objednatelem, zejména dokumentace přiložené k žádosti o podporu a výsledků probíhající Analýzy rizik (včetně skenu zranitelnosti). Zhotovitel tedy

¹⁾ Zejména: zákon č. 365/2000 Sb., o informačních systémech veřejné správy v aktuálním znění (verze 37), §1 a §14 zákona č. 264/2025 Sb. o kybernetické bezpečnosti a §16 vyhlášky č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.

²⁾ §1, písm. b) vyhlášky č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat

nebude povinen provádět zpětné testování stavu před implementací opatření.

4. Termíny plnění

- 4.1. Zhotovitel bude plnit své povinnosti průběžně tak, aby bylo řádně a včas v dohodnutých termínech dosaženo účelu této smlouvy.
- 4.2. Zhotovitel zahájí plnění povinností podle této smlouvy bez zbytečného odkladu po nabytí její účinnosti při dodržení níže uvedeného harmonogramu:
- 4.3. **Realizace** (tj. provedení auditu kybernetické bezpečnosti včetně zpracování dokumentace systému řízení bezpečnosti) bude zahájena ihned po nabytí účinnosti této smlouvy.

Výstupy realizace

- a) budou splňovat náležitosti a budou vypracovány v rozsahu stanoveném v Příloze č. 1 této smlouvy,
 - b) budou vyhotoveny v českém jazyce a bez vad a nedodělků předány Objednateli ve dvou vyhotoveních v listinné podobě s podpisem osob oprávněných zastupovat ve věci plnění této smlouvy Zhotovitele a v jednom vyhotovení v elektronické podobě v editovatelném formátu.
- 4.4. **Dokončení realizace**, (tj. předání auditu kybernetické bezpečnosti, vykonání penetračních testů a vyhodnocení zvýšení kyberbezpečnosti – dále jen "Výstupy realizace") Objednateli proběhne **nejpozději do 5. prosince 2025**.
 - 4.5. Zhotovitel je povinen před předáním plnění díla a jeho převzetím Objednatelem s ním předem projednat veškeré své předkládané závěry.
 - 4.6. Smluvní strany se zavazují jednat efektivně a vstřícně k požadavkům druhé strany tak, aby **konečné verze Výstupů realizace byly** předány Zhotovitelem a **převzaty Objednatelem nejpozději do 20. prosince 2025**.
 - 4.7. Postup předání plnění:
 - a) Objednatel se seznámí se Zhotovitelem předanými Výstupy realizace a do deseti (10) kalendářních dnů od jejich převzetí sdělí Zhotoviteli své připomínky k auditu či návrhy na jeho doplnění a oznámí Zhotoviteli případné vady.
 - b) Zhotovitel je povinen Objednatelem sdělené připomínky a návrhy na doplnění Výstupů realizace vypořádat a odstranit případně oznámené vady Výstupů realizace bez zbytečného odkladu tak, aby úplné a konečné verze Výstupů realizace předal a Objednatel převzal nejpozději do 15 kalendářních dnů od 1. (prvního) předání Výstupů realizace Objednateli.
 - 4.8. Ověření správnosti údajů uvedených v auditu kybernetické bezpečnosti bude zahrnovat ověření, zda informace v tomto auditu zohledňují všechny podstatné údaje, které Zhotovitel získal analýzou prostředí Objednatele, a zda jsou uvedeny srozumitelně, věcně správně, v potřebném rozsahu a nezavádějícím způsobem a zda plně korespondují s poznatky, které Zhotoviteli při plnění této smlouvy poskytl Objednatel.
 - 4.9. Podmínkou pro řádné splnění povinnosti Zhotovitele, (tj. k předložení Výstupů realizace), je včasné splnění povinnosti Objednatele k poskytnutí součinnosti dle požadavků ve smyslu odst. 4.6. a 4.7. této smlouvy. O dobu prodlení s plněním této povinnosti Objednatele se prodlužuje i termín pro předložení Výstupů realizace Zhotovitelem Objednateli.
 - 4.10. Smluvní strany sepiší o předání a převzetí Výstupů realizace písemný předávací protokol.

5. Součinnost

- 5.1. Objednatel poskytne Zhotoviteli při získávání potřebných informací nezbytnou součinnost svých pracovníků a dále:

- a) přístup k relevantním dokumentům a svojí existující provozní dokumentací³⁾,
 - b) zodpovězení všech dotazů Zhotovitele týkajících se relevantních skutečností vztahujících se k Objednatelem používaným informačním a komunikačním technologiím a systémům včetně systémové architektury a jeho existujících bezpečnostních politik.
- 5.2. Zhotovitel konkretizuje soupis svých Požadavků na součinnost Objednatele (dále též jen „Požadavky“) a Objednateli zašle nejpozději do osmi (8) pracovních dnů od účinnosti smlouvy. Tyto Požadavky nesmějí být nepřiměřené a nesmějí zatížit Objednatele jakýmkoliv náklady nad rámec obvyklých mzdových nákladů spojených s činností zaměstnanců a dalších pracovníků Objednatele. Zhotovitel bere na vědomí a souhlasí, že Objednatel může podmínit poskytnutí vyžádaných podkladů či informací přijetím odpovídajících opatření a záruk na straně Zhotovitele (včetně jeho poddodavatelů, zaměstnanců a spolupracujících osob) k ochraně důvěrných či citlivých informací včetně uzavření samostatných dohod o ochraně důvěrných informací.
- 5.3. Objednatel předloží své stanovisko k Požadavkům do osmi (8) pracovních dnů od jejich předložení Zhotovitelem, a to společně se svými připomínkami a návrhy na úpravy zajištění Požadavků.
- 5.4. Smluvní strany se zavazují jednat efektivně a vstřícně k požadavkům druhé strany tak, aby byl soupis Požadavků schválen nejpozději do osmnácti (18) pracovních dnů od účinnosti smlouvy.

6. Povinnosti Zhotovitele

- 6.1. Zhotovitel je povinen při plnění svých povinností dodržovat příslušná ustanovení obecně závazných právních předpisů a jiných standardů týkajících se jeho odborné a profesní činnosti, (zejména pokud jde o povinnosti stanovené zákonem č. 264/2025 Sb., o kybernetické bezpečnosti, zákonem č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, včetně prováděcích předpisů k těmto zákonům, mezinárodně uznávané standardy kybernetické bezpečnosti a opatření, doporučení a stanoviska Národního úřadu pro kybernetickou a informační bezpečnost).
- 6.2. Zhotovitel při plnění smlouvy bude postupovat:
- a) v souladu se smlouvou a v ní stanoveném rozsahu, tedy tak, aby o prostředí Objednatele získal dostatečné a potřebné informace, které mu umožní objektivně zhodnotit (posoudit) úroveň rizik pro kybernetickou a informační bezpečnost prostředí Objednatele a navrhnout odpovídající opatření pro předcházení vzniku těchto rizik a jejich eliminaci,
 - b) tak, aby získal dostatečné a potřebné informace, které mu umožní provést audit kybernetické bezpečnosti v souladu s touto smlouvou a v rozsahu stanoveném touto smlouvou. Při získávání informací vztahujících se k provádění auditu kybernetické bezpečnosti poskytne Objednatel Zhotoviteli potřebnou součinnost a je povinen předložit mu dokumenty a sdělit informace týkající se všech skutečností relevantních pro provedení auditu kybernetické bezpečnosti. Smluvní ujednání o ochraně důvěrných informací tímto odstavcem smlouvy nejsou nijak dotčena. Zhotovitel se zavazuje při provádění Díla postupovat ve vzájemné součinnosti s dodavatelem dalších částí veřejné zakázky tak, aby bylo dosaženo účelu této smlouvy.
 - c) ve vzájemné součinnosti s Objednatelem, a to včetně pravidelného (každý týden) projednávání veškerých zjištěných dílčích závěrů a navrhovaných doporučení. Uvedené projednávání bude mít za cíl operativně (bez zbytečných odkladů) ověřovat správnost a úplnost (zda informace zohledňují všechny podstatné údaje) Zhotovitelem v prostředí Objednatele zjištěných údajů, a zda jsou uvedeny srozumitelně, věcně správně, v potřebném rozsahu a nezavádějícím způsobem a zda plně korespondují s poznatky, které Zhotoviteli při plnění smlouvy poskytl Objednatel.
- 6.3. Aby Objednatel mohl poskytovat Zhotoviteli smluvní součinnost včas je Zhotovitel povinen si ji od Objednatele vyžádat s dostatečným časovým předstihem.

³⁾ Ve smyslu vyhlášky č. 529/2021 Sb., o povinné dokumentaci informačního systému veřejné správy



- 6.4. Pokud se na tom smluvní strany následně dohodnou a pokud to bude možné s ohledem na předpisy upravující zadávání veřejných zakázek, bude Zhotovitel po splnění závazku dle smlouvy pro Objednatele provádět průběžné konzultace a poradenskou činnost v oblasti kybernetické a informační bezpečnosti.
- 6.5. Zhotovitel zajistí, že výkon role hlavního autora plnění projektu bude vykonávat osoba, která je držitelem potřebné (požadavky legislativy splňující) certifikace.
- 6.6. Zhotovitel je povinen:
- ověřit a zajistit, že jím zhotovený audit kybernetické bezpečnosti podává věrný a úplný obraz o stavu a úrovni informačních a komunikačních systémů a technologií Objednatele,
 - vyhodnotit rizika pro kybernetickou a informační bezpečnost v prostředí Objednatele a navrhnout vhodná opatření pro předcházení a eliminaci těchto rizik včetně adekvátních opatření pro pořízení nových informačních a komunikačních technologií Objednatelem k naplnění tohoto účelu,
 - neprodleně informovat o zjištěných nedostatcích týkajících se plnění předmětu této smlouvy, zejména pokud jde o nedostatky při poskytování součinnosti ze strany Objednatele. Zhotovitel bude v návaznosti na svá zjištění informovat Objednatele o navrhovaných postupech ke zlepšení a zefektivnění smluvní spolupráce.
 - mít uzavřeno pojištění odpovědnosti za újmu způsobenou v souvislosti s poskytováním služeb podle této smlouvy s limitem pojistného plnění nejméně ve výši odměny dle čl. 8.1. této smlouvy. Zhotovitel prohlašuje, že má takové pojištění uzavřeno a že jej bude udržovat po celou dobu plnění této smlouvy v platnosti, a zavazuje se na požádání Objednatele existenci takového pojištění prokázat.
- 6.7. Zhotovitel zpracuje audit kybernetické bezpečnosti a na jeho základě zpracuje a předloží své názory a doporučení k zajištění odpovídající úrovně kybernetické a informační bezpečnosti v prostředí Objednatele. Zhotovitel ověří informace potřebné pro řádné a úplné vypracování auditu kybernetické bezpečnosti. Zhotovitel při plnění svých povinností posuzuje významné hrozby pro kybernetickou a informační bezpečnost v prostředí Objednatele, které by mohly ohrozit či narušit provoz Objednatele a plnění jeho hlavního předmětu činnosti. Zhotovitel přitom vychází z analýzy prostředí Objednatele a hrozeb pro kybernetickou a informační bezpečnost, které by se mohly projevit v prostředí Objednatele. Povinností Zhotovitele je postupovat v souladu s obecně uznávanými postupy a doporučeními tak, aby získal všechny informace, které jsou podle jeho nejlepšího vědomí potřebné pro komplexní audit prostředí Objednatele z pohledu kybernetické a informační bezpečnosti a poskytují odpovídající záruku, že v prostředí Objednatele budou implementována taková opatření, která umožní dosáhnout co nejvyšší úrovně kybernetické a informační bezpečnosti v prostředí Objednatele při zohlednění finančních a ekonomických možností Objednatele.
- 6.8. Veškeré činnosti dle této smlouvy bude Zhotovitel provádět tak, aby získal potřebné informace o prostředí Objednatele a mohl posoudit úroveň rizik pro kybernetickou a informační bezpečnost prostředí Objednatele a v souladu s tím navrhnout odpovídající opatření pro předcházení vzniku těchto rizik a jejich eliminaci.
- 6.9. Zhotovitel bude pro Objednatele provádět po splnění závazku dle této smlouvy průběžné konzultace a poradenskou činnost v oblasti kybernetické a informační bezpečnosti, pokud se na tom smluvní strany následně dohodnou a pokud to bude možné s ohledem na předpisy upravující zadávání veřejných zakázek.

7. Povinnosti Objednatele

- 7.1. Objednatel je ve smyslu smlouvy povinen poskytnout Zhotoviteli potřebnou součinnost při získávání informací potřebných pro hodnocení kybernetické bezpečnosti svých informačních aktiv.



- 7.2. Objednatel Zhotoviteli na jeho vyžádání zpřístupní Zhotoviteli v nezbytném rozsahu svoji existující provozní dokumentaci⁴⁾ vztahující se k jím používaným informačním a komunikačním technologiím a systémům včetně systémové architektury a existujících bezpečnostních politik. Zpřístupnění dokumentace se uskuteční podle konkrétně dohodnutých podmínek formou protokolu spolu s uvedením informací a podkladů, které jsou Zhotoviteli zpřístupněny. Objednatel se zavazuje zajistit nezbytnou součinnost členů statutárního orgánu Objednatele a dalších dotčených pracovníků, zejména věcných správců předmětných informačních systémů Objednatele a pracovníků oddělení informatiky.
- 7.3. Objednatel se zavazuje poskytnout Zhotoviteli k provedení auditu dokumentaci, která byla přiložena k žádosti o podporu, a dále výsledky probíhající Analýzy rizik (včetně skenu zranitelností).

8. Odměna Zhotovitele

- 8.1. Zhotoviteli náleží za splnění jeho povinností dle této smlouvy odměna ve výši 398.000,- Kč (slovy třístadevadesátosm tisíc korun českých) bez DPH. K této odměně bude připočtena daň z přidané hodnoty podle sazby platné ke dni uskutečnění zdanitelného plnění.
- 8.2. Odměna uvedená v odst. 8.1. této smlouvy náleží Zhotoviteli za úplné a řádné (bezvadné) splnění jeho povinností podle této smlouvy ve smyslu článku 3.
- 8.3. V odměně Zhotovitele jsou zahrnuty veškeré náklady, které Zhotoviteli při plnění jeho povinností dle této smlouvy vzniknou, včetně nákladů na pracovníky Zhotovitele, jeho poddodavatele a spolupracující osoby, cestovní výdaje, výdaje spojené s ubytováním, náklady na pojištění atd. Zhotovitel není oprávněn domáhat se po Objednateli úhrady jakýchkoliv dalších nákladů nebo hotových výdajů. V odměně Zhotovitele jsou zahrnuty i činnosti, které nejsou výslovně uvedeny v této smlouvě, které jsou však k řádnému provedení díla nezbytné a o kterých Zhotovitel vzhledem ke své kvalifikaci a zkušenostem měl nebo mohl vědět.
- 8.4. Právo Zhotovitele na vyúčtování odměny za splnění jeho smluvní povinností vznikne dnem řádného a úplného předání a převzetí smluvního plnění bez vad a nedodělků akceptačním protokolem.
- 8.5. Smluvní odměnu Objednatel uhradí na základě řádně vystavené faktury Zhotovitele.
- 8.6. Odměna se považuje za zaplacenou v okamžiku, kdy byla příslušná částka odepsána z účtu Objednatele ve prospěch účtu Zhotovitele. Zhotovitel není oprávněn požadovat po Objednateli žádné zálohy. Odměna bude hrazena na účet Zhotovitele uvedený na prokazatelně Objednateli doručené faktuře.
- 8.7. Zhotovitel je povinen vystavit fakturu nejdříve dnem, kdy mu vzniklo právo na odměnu. Splatnost faktury je třicet (30) dnů od jejího prokazatelného doručení Objednateli.
- 8.8. Faktura Zhotovitele musí obsahovat minimálně následující údaje: názvy smluvních stran a adresy jejich sídla, IČ a DIČ smluvních stran, číslo faktury, den vystavení a den splatnosti faktury, den uskutečnění zdanitelného plnění, označení peněžního ústavu a číslo účtu, na který se má platit v souladu s touto smlouvou, fakturovanou částku, podpis oprávněné osoby a případně další náležitosti stanovené příslušnými právními předpisy. Faktura bude rovněž obsahovat název projektu, registrační číslo projektu a informaci, že se jedná o projekt podpořený z Národního plánu obnovy, a to následujícím způsobem: **Projekt „Zvýšení kybernetické bezpečnosti pro infrastrukturu města Telč“, reg. č. CZ.31.2.0/0.0/0.0/23_093/0008474, je spolufinancován z Národního plánu obnovy“.**
- 8.9. Nebude-li faktura obsahovat stanovené náležitosti, nebo v ní nebudou správně uvedené údaje dle této smlouvy, je Objednatel oprávněn fakturu vrátit ve lhůtě deseti (10) dnů od jejího obdržení Zhotoviteli. V takovém případě se přeruší běh lhůty splatnosti a nová lhůta splatnosti počne běžet prokazatelným doručením opravené faktury.

⁴⁾ Ve smyslu vyhlášky č. 529/2021 Sb., o povinné dokumentaci informačního systému veřejné správy



- 8.10. Zhotovitel vystaví fakturu v elektronické formě ve formátu PDF a v této formě ji odešle do datové schránky Objednatele. Faktura odeslaná v rozporu s tímto požadavkem nebude považována za doručenou.

9. Odstoupení od smlouvy

- 9.1. Smluvní strany mohou odstoupit od smlouvy z důvodů upravených v příslušných právních předpisech nebo uvedených v této smlouvě. Odstoupení musí být učiněno v písemné formě a musí být prokazatelně doručeno druhé smluvní straně.
- 9.2. Objednatel je oprávněn odstoupit od smlouvy v případě, že se Zhotovitel ocitne v situaci, ohrožující řádné plnění povinností ze smlouvy, tedy zejména v případě zrušení Zhotovitele bez právního nástupce, úpadku Zhotovitele, zahájení insolvenčního řízení se Zhotovitelem nebo ztráty nebo pozastavení oprávnění k výkonu činnosti, která je předmětem této smlouvy. Objednatel je rovněž oprávněn odstoupit od smlouvy v případě, že průběžné plnění povinností Zhotovitele bude vyvolávat důvodné pochybnosti Objednatele o řádném a včasném dokončení povinností Zhotovitele, zejména pokud jde o předložení auditu kybernetické bezpečnosti, a Zhotovitel v poskytnuté lhůtě v délce nejméně deseti (10) dnů nezjedná nápravu vytýkaných nedostatků v postupu plnění jeho povinností. Objednatel je rovněž oprávněn odstoupit od smlouvy v případě prodlení Zhotovitele s předložením auditu kybernetické bezpečnosti dle odst. 4.6. této smlouvy po dobu nejméně deseti (10) dnů.
- 9.3. Odstoupení od smlouvy nabývá účinnosti dnem doručení oznámení o odstoupení druhé smluvní straně a k tomuto datu zanikají práva a povinnosti z ní vyplývající.

10. Odpovědnost za újmu a sankce

- 10.1. Smluvní strany si vzájemně odpovídají za újmu (včetně újmy nemajetkové), kterou způsobí druhé smluvní straně porušením dohodnutých nebo zákony ČR stanovených povinností.
- 10.2. Každá ze smluvních stran je povinna předcházet vzniku újmy, učinit vhodná a přiměřená opatření k odvrácení hrozící újmy a v případě jejího vzniku učinit veškerá rozumně požadovatelné kroky vedoucí k tomu, aby rozsah škody byl co možná nejmenší. Současně s tím je povinna nahradit újmu (včetně újmy nemajetkové), která druhé smluvní straně vznikla.
- 10.3. Zhotovitel je povinen zaplatit Objednateli smluvní pokutu ve výši 5.000,- Kč (slovy Pět tisíc korun českých) za každý započatý kalendářní den prodlení s předložením auditu kybernetické bezpečnosti ve smyslu článku 4 této smlouvy. Právo na náhradu způsobené škody tím není dotčeno.
- 10.4. Zhotovitel se zavazuje plnit povinnosti, jejichž splnění je sankcionované smluvní pokutou, i po zaplacení smluvní pokuty.
- 10.5. Ujednání o smluvní pokutě nebo zaplacení smluvní pokuty nezabavuje Zhotovitele povinnosti k náhradě újmy (včetně újmy nemajetkové) způsobené Objednateli porušením povinností sankcionované smluvní pokutou. Za újmu se považují také veškeré sankční platby, které bude Objednatel povinen uhradit orgánům veřejné moci v souvislosti s porušením povinností Objednatele, zapříčiněné porušením povinností Zhotovitele dle této smlouvy.
- 10.6. Smluvní pokuta je vždy splatná nejpozději do sedmi (7) dnů poté, co Objednatel požádá Zhotovitele o zaplacení smluvní pokuty.
- 10.7. Smluvní strany se zavazují zaplatit druhé smluvní straně úrok z prodlení ve výši 0,05 % z dlužné částky za každý, byť započatý den prodlení se splněním své peněžité povinnosti dle této smlouvy.
- 10.8. Za porušení právní povinnosti ve smyslu této smlouvy se rovněž považuje, jestliže se některé prohlášení Zhotovitele, učiněné v této smlouvě, ukáže být nepravdivým, nepřesným či zavádějícím (dále též jen „Porušení prohlášení“). Zhotovitel se zavazuje nahradit Objednateli újmu (včetně újmy nemajetkové), která mu vznikne v příčinné souvislosti s Porušením prohlášení, neboť Porušení prohlášení se považuje za porušení povinností Zhotovitele jednat



poctivě, čestně, svědomitě, s péčí řádného hospodáře a v souladu se zásadami poctivého obchodního styku a dále za porušení povinnosti Zhotovitele předcházet hrozícím újmám.

11. Komunikace a jednání smluvních stran

11.1. Má-li být dle této smlouvy doručeno oznámení, žádost či jiné sdělení druhé smluvní straně v písemné formě, zašle odesílající strana tuto záznam datovou schránkou. Pro běžnou komunikaci v rámci spolupráce, předávání podkladů, dílčích výstupů apod. strany ujednaly využít portál Zhotovitele na adrese <https://xr.elat.cz>.

11.2. V případě, že adresát zásilky odmítne tuto bezdůvodně převzít, má se za to, že zásilka byla doručena dnem, kdy byla bezdůvodně odmítnuta. V případě, že zásilka bude uložena pro adresáta u osoby pověřené jejím doručením, má se za to, že zásilka byla doručena třetí (3.) den po jejím uložení.

11.3. Smluvní strany uvedly za účelem doručování následující kontaktní údaje:

Objednatel: Město Telč
ISDS: c26bg9k
E-mail: [REDACTED]
Telefon: [REDACTED]

Zhotovitel:
ISDS twv3hij
E-mail: [REDACTED]
Telefon: [REDACTED]

11.4. Smluvní strany tímto jmenují a pověřují osoby oprávněné vzájemně jednat v záležitostech týkajících se plnění této smlouvy:

- za Objednatele bude jednat ve věci plnění této smlouvy jako zástupce:

o [REDACTED]

- za Zhotovitele bude jednat ve věci plnění této smlouvy jako zástupce:

o Lukáš Vondráček, jednatel společnosti, [REDACTED]

11.5. Smluvní strany se dohodly, že veškerá písemná oznámení, žádosti či sdělení dle této smlouvy budou činěna v českém jazyce. V českém jazyce bude probíhat též jiná komunikace mezi smluvními stranami vedená v souvislosti s touto smlouvou.

11.6. Smluvní strany se zavazují, že oznámí neprodleně druhé smluvní straně změnu jakéhokoliv z výše uvedených kontaktních údajů či změnu pověřených osob ve smyslu odst. 11.4. této smlouvy. Tyto změny nepodléhají schválení druhou smluvní stranou a nepovažují se za změnu této smlouvy ve smyslu odst. 13.4. této smlouvy.

11.7. Smluvní strany se dohodly na vytvoření pracovního týmu (dále též jen „Projektový tým“), který bude vzájemně úzce spolupracovat při plnění technických, provozních či organizačních úkolů dle této smlouvy a účastnit se pravidelných koordinačních schůzek. Ze strany Objednatele budou tvořit Projektový tým pověřená osoba dle odst. 11.4. této smlouvy, zaměstnanci oddělení informatiky a další pověřené osoby podílející se na plnění úkolů Objednatele v oblasti kybernetické bezpečnosti, přičemž osobou pověřenou v rámci Projektového týmu ke koordinaci jednotlivých úkolů a komunikaci se Zhotovitelem je pověřená osoba dle odst. 11.4. této smlouvy. Ze strany Zhotovitele tvoří Projektový tým pověřená osoba dle odst. 11.4. této smlouvy a dále osoby uvedené v nabídce Zhotovitele k této věci, přičemž osobou pověřenou v rámci Projektového týmu ke koordinaci jednotlivých úkolů a komunikaci s Objednatelem je pověřená osoba dle odst. 11.4. této smlouvy. Každá smluvní strana je oprávněna označit další osoby, které budou členy Projektového týmu, a osoby pověřené plněním jejich jednotlivých technických, provozních či organizačních úkolů. Jakoukoliv změnu ve složení těchto osob je každá smluvní strana povinna předem písemně oznámit druhé smluvní straně, aniž by se to považovalo za změnu této smlouvy.



- 11.8. Projektový tým především řeší a projednává běžné technické, provozní a organizační úkoly, otázky a problémy, ke kterým obvykle dochází při správě, provozu a podpoře informačních a komunikačních systémů a souvisejících informačních a komunikačních technologií (včetně výpočetní techniky) a které mají dopady do oblasti kybernetické bezpečnosti.

12. Ochrana informací

- 12.1. Smluvní strany se zavazují zachovávat mlčenlivost o všech skutečnostech a informacích, o kterých se dozvěděly v souvislosti s touto smlouvou. Povinnost mlčenlivosti se nevztahuje na ty skutečnosti, které jsou nebo se stanou obecně známými, aniž by se tak stalo v důsledku porušení této smlouvy nebo je povinnost zveřejnění stanovena zákonem.
- 12.2. Objednatel má především zájem na ochraně důvěrnosti informací, které mají dopad na kybernetickou a informační bezpečnost v prostředí Objednatele, včetně informací o informačních a komunikačních systémech a technologiích Objednatele, způsobech jejich ochrany a zabezpečení, o obsahu bezpečnostních politik a dalších interních dokumentů Objednatele upravujících oblast informačních a komunikačních systémů a technologií, a dále má zvláštní zájem na ochraně důvěrnosti informací, které takto budou Objednatelem výslovně označeny.
- 12.3. Omezení stanovená v odst. 12.1. a odst. 12.2. této smlouvy se nevztahují na poskytování informací spolupracujícím osobám a/nebo konzultantům obou smluvních stran v nezbytném rozsahu, pokud tyto spolupracující osoby a/nebo konzultanti budou zavázáni k ochraně informací nejméně ve stejném rozsahu jako smluvní strany.
- 12.4. Smluvní strany jsou však oprávněny podávat potřebná vysvětlení a údaje příslušným oprávněným státním a veřejným úřadům a institucím v České republice a/nebo oprávněným veřejným úřadům a institucím Evropské unie, jakož i plnit oznamovací povinnosti a uveřejňovat údaje, dokumenty a informace, pokud jsou k tomu povinny dle příslušných obecně závazných právních předpisů.
- 12.5. Získá-li některá smluvní strana od druhé smluvní strany dokumenty, které obsahují skutečnosti či informace chráněné dle tohoto článku smlouvy (bez ohledu na jejich formu, která může být listinná či elektronická) je tato smluvní strana povinna zajistit bezpečné uložení těchto dokumentů tak, aby nemohlo dojít k prozrazení či zneužití chráněných skutečností či informací.
- 12.6. Smluvní strany se zavazují dodržovat povinnosti uvedené v tomto článku smlouvy po celou dobu trvání smlouvy i po dobu od ukončení této smlouvy.
- 12.7. Zhotovitel se výslovně zavazuje:
- nepořizovat kopie z dokumentace zpřístupněné mu Objednatelem v rámci povinné součinnosti a veškerou zapůjčenou dokumentaci Objednateli vrátit nejpozději k datu ukončení smlouvy
 - zachovávat mlčenlivost o všech osobních údajích a/nebo jiných údajích chráněných zvláštními právními předpisy, se kterými se případně dostane do styku při plnění této smlouvy. Při nakládání s osobními údaji a/nebo jinými údaji chráněnými zvláštními právními předpisy, se kterými se případně Zhotovitel dostane do styku při plnění této smlouvy, je vždy rozhodujícím hlediskem ochrana práv a zájmů Objednatele.

13. Závěrečná ustanovení

- 13.1. Smluvní strany prohlašují, že si tuto smlouvu přečetly, že s jejím obsahem souhlasí a že vyjadřuje jejich pravou, svobodnou a vážnou vůli. Dále prohlašují, že ji neuzavřely v tísní, ani za nápadně nevýhodných podmínek. Na důkaz toho připojují jejich oprávnění zástupci své vlastnoruční podpisy.
- 13.2. Pokud v této smlouvě není stanoveno jinak, řídí se právní vztahy z ní vzniklé právním řádem České republiky, zejména zákonem č. 89/2012 Sb., občanským zákoníkem, ve znění pozdějších předpisů.



- 13.3. Tato smlouva představuje úplnou dohodu smluvních stran o předmětu této smlouvy a nahrazuje veškerá předešlá ujednání smluvních stran ústní i písemná týkající se předmětu této smlouvy.
- 13.4. Tato smlouva může být měněna pouze písemnými, vzestupně číslovanými dodatky, uzavřenými na základě dohody obou smluvních stran.
- 13.5. Neplatnost, neúčinnost či nevymahatelnost jednotlivého ustanovení této smlouvy, nezpůsobuje neplatnost, neúčinnost či nevymahatelnost smlouvy jako celku. Smluvní strany se zavazují takové ustanovení nahradit bez zbytečného odkladu jiným ustanovením, které bude platné, účinné a vymahatelné a které svým obsahem bude nejvíce odpovídat smyslu a účelu původního ustanovení této smlouvy.
- 13.6. Smluvní strany se zavazují řešit případné spory vzniklé z této smlouvy smírem v souladu s účelem této smlouvy. Dožádaná smluvní strana je povinna se zúčastnit jednání o vyřešení sporu do jednoho (1) týdne od požádání druhou smluvní stranou. Nepodaří-li se vyřešit případný spor smírnou cestou, bude předložen jednou ze Stran obecnému soudu Objednatel.
- 13.7. Zhotovitel je povinen uvádět povinné prvky publicity podle podmínek strukturálních fondů EU na všech tištěných dokumentech vytvořených v souvislosti s předmětem této smlouvy (nevztahuje se na interní účetní dokumentaci apod.). Tyto povinné prvky publicity sdělí a poskytne Zhotoviteli na vyžádání Objednatel.
- 13.8. Zhotovitel je povinen při kontrole poskytnout na vyžádání kontrolnímu orgánu daňovou evidenci v plném rozsahu. Zhotovitel 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), ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly.
- 13.9. Zhotovitel je povinen minimálně do konce roku 2037 poskytovat požadované informace a dokumentaci související s realizací projektu, z něhož je Veřejná zakázka hrazena, zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost.
- 13.10. Zhotovitel bere na vědomí, že úhrada ceny za předmět plnění bude provedena s využitím dotačních prostředků získaných Objednatel a podléhajících kontrole z hlediska vykazování účelnosti jejich čerpání. Zhotovitel se zavazuje, že Objednateli nahradí veškeré škody a náklady, které mu vzniknou nebo budou muset být vynaloženy, pokud z důvodu porušení této smlouvy Zhotovitelem vznikne Objednateli závazek vrátit dotaci nebo její část poskytnutou na úhradu ceny za předmět plnění jejímu poskytovateli, a to včetně penále případně vyměřeného jako důsledek porušení pravidel nakládání s veřejnými prostředky. To platí obdobně, pokud Zhotovitel znemožní řádný výkon kontroly orgánům oprávněným ke kontrole účelnosti vynaložení dotačních prostředků, resp. nepředloží jimi požadované doklady.
- 13.11. Nedílnou součástí této smlouvy je její Příloha č. 1 – "**Podrobnější informace o zakázce**". Smluvní strany prohlašují, že se s touto přílohou řádně seznámily a že porozuměly jejímu obsahu.
- 13.12. Tato smlouva je podepsána v souladu s podmínkami stanovenými zákonem o zadávání veřejných zakázek v platném znění elektronicky.
- 13.13. Smlouva nabývá platnosti dnem podpisu a účinnosti dnem jejího uveřejnění v registru smluv, které zajistí Objednatel.

Zhotovitel:

Objednatel:

V _____ dne _____

V Telči dne dle data el. podpisu



Financováno
Evropskou unií
NextGenerationEU



NÁRODNÍ
PLÁN OBNOVY

.....
Lukáš Vondráček,
Jednatel společnosti
ELAT, s.r.o.

.....
Mgr. Vladimír Brtník, starosta
Město Telč

Příloha č. 1

Podrobnější informace o zakázce:

„Pořízení auditu kybernetické bezpečnosti“

1. Zaměření Auditů je:

- primárně na informační systémy:
 - IS GINIS – komplexní agendový informační systém zajišťující podporu práce městského úřadu. Uživateli IS je cca 70, správce 1, provoz a správa IS je řešena interně.
 - IS VITA – agendový informační systém na poli stavebního řádu. Uživateli IS je cca 7, správce 1, provoz a správa IS je řešena interně.
- následně na všechna informační aktiva Objednatele včetně jeho klíčových procesů a hlavních provozních operací organizace, tzn. bude zpracován tak, aby obsáhl všechny oblasti činnosti Objednatele, které využívají podporu IT, a to jak interně poskytovanou (využívající jak organizační, tak i technická aktiva Objednatele v rámci jeho interního prostředí), tak smluvně zajišťovanou externími dodavateli.

2. Audit organizačních aktiv

- 2.1. U organizačních aktiv Audit zhodnotí primárně správnost a komplexnost procesních pravidel a **respektování** nastavených přístupových oprávnění.
- 2.2. Výstupem Auditů bude hodnotící zpráva, zpracovaná na základě bezpečnostních testů, dotazníkových šetření a fyzického ověření, V uvedeném zhodnocení Zhotovitel zohlední i kompetence a kompetentnost uživatelů (včetně případných externích) v jednotlivých rolích:
 - věcného správce (kybernetické) bezpečnosti úřadu / objednatel,
 - oddělení informatiky úřadu,
 - běžný uživatel (referent).
- 2.3. Všechny výstupy plnění Zhotovitel dodá standardně i na elektronickém médiu, a to včetně výstupů z v rámci Auditů použitých nástrojů a případných doplňujících informací z testům (např. screenshoty z průběhu testů).

3. Struktura výstupu

- 3.1. Hodnotící zprávu Auditů Objednatel požaduje v následujícím členění:

- A. souhrnná část kompletně shrnující veškeré body plnění,
- B. Manažerské shrnutí rekapitulující stručně – v bodech zjištění podrobně popsaná v části 1,
- C. přílohy.

Ad A. - souhrnná část závěrečné hodnotící zprávy

Tato část zprávy představuje faktické těžiště zakázky. Pro větší přehlednost ji Objednatel požaduje zpracovat ve struktuře shodné s předmětem plnění dle bodu 3.2 smlouvy, tzn. v členění na tyto dílčí kapitoly:

Kapitola I. audit kybernetické bezpečnosti ve smyslu zákonné povinnosti,

Kapitola II. zjištění faktického aktuálního stavu kybernetické bezpečnosti digitálního prostředí Objednatele ve společné synergii výstupů částí č 1 až 9 projektu: „Zvýšení kybernetické bezpečnosti pro infrastrukturu města Telče“ a

Kapitola III. Vyhodnocení, jak výše uveden projekt (jako celek, tj. všech jeho devět částí) skutečně zvýšil kybernetickou bezpečnost Objednatele a konkrétní specifikace

případných nedostatků aktuálního stavu kybernetické bezpečnosti Objednatele, jejich prioritizace dle závažnosti a návrh konkrétních opatření⁵⁾ k nápravě.

Ad. Kap. I. - audit kybernetické bezpečnosti ve smyslu zákonné povinnosti

Rozsah, zaměření a způsob auditu kybernetické bezpečnosti Objednatele zpracuje Zhotovitel v souladu se zákonnými povinnostmi Objednatele.

Závěrečná zpráva z tohoto auditu bude zpracována formou posudku nezávislého certifikovaného auditora a do zprávy začleněna ve formě přílohy, tj. jako samostatného dokumentu.

Ad. Kap. II.

Zjišťování aktuálního stavu informačních aktiv Objednatele, tj. objektivní testování a analýzu, provede Zhotovitel fyzickou kontrolou a praktickým testováním implementovaných opatření na místě, a to dle rozsahu, který je definován zadávací dokumentací částí 1 až 8 a 11 projektu „**Zvýšení kybernetické bezpečnosti pro infrastrukturu města Telče**“, reg. č. CZ.31.2.0/0.0/0.0/23_093/0008474, je spolufinancován z Národního plánu obnovy“.. včetně vyhodnocení dodržování upravených interních procesů a reálného využívání funkcionalit technologií pořízených a zavedených v rámci realizace částech 1. až 8. a 11. projektu, tzn. po realizaci / implementaci následujících bezpečnostní opatření:

- a) **organizačních**, tj. po zavedení dokumentace systému řízení bezpečnosti informací (pořízené v rámci části 1: *Analýza rizik a další dokumentace systému řízení bezpečnosti informací projektu*), jako závazných interních procesních pravidel,
- b) **technických**, tj. po nasazení následujících klíčových prvků technologického řešení (v rámci částí 2. až 8. projektu):
 - Zabezpečení komunikační sítě v rozsahu L2/L3 switche a nástroje pro segmentaci datové komunikační sítě, NAC, 802.1X (§18)
 - Pořízení a implementace nástroje pro multifaktorovou autentizaci (§19)
 - Dodávka a implementace nástroje pro řízení přístupů a identit (§20; §22)
 - Pořízení a implementace nástroje pro analýzu a monitoring síťového provozu (§23).
 - Pořízení a implementace nástroje pro správu aktiv a řízení rizik a zranitelností (§24)
 - Pořízení a implementace nástroje pro log management (§24)
 - Pořízení a implementace nástroje pro Mobile/Enterprise device management (§25)
 - Zálohování a archivace (§25; §27).

Podrobněji o testování viz bod 4. Přílohy

Ad. Kap. III.

V této kapitole Zhotovitel zhodnotí / porovná, zda aktuální stav kybernetické bezpečnosti městského úřadu Telče dle provedených zjištění je v souladu s cíli zadání výše zmíněného projektu: „**Zvýšení kybernetické bezpečnosti pro infrastrukturu města Telče**“.

Podrobněji o testování viz bod 5. Přílohy

4. Testování

4.1. Hlavní cíle testování:

- ověřit správnou implementaci opatření dodaných v rámci projektu: „Zvýšení kybernetické bezpečnosti pro infrastrukturu města Telče“ jako celku, tj. prokázat, že po jeho realizaci aktuálně jako nevyřešená zůstala pouze akceptovatelná rizika⁶⁾.

⁵⁾ §1, písm. b) vyhlášky č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat

⁶⁾ § 2, písm. b) vyhlášky č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat

- odhalit případné zranitelnosti jak v interním, tak externím prostředí.
- zkontrolovat, zda konfigurace odpovídají doporučeným bezpečnostním postupům.
- prověřit funkčnost klíčových bezpečnostních mechanismů, jako jsou přihlášení, VPN nebo síťová segmentace.

4.2. Zhotovitel provede:

- vnější penetrační testy vůči z vnějšku dostupným systémům Objednatele ze svého sídla bez ohledu na jejich místo provozu (cloud, jiný poskytovatel, in-house).
Seznam IP adres a identifikace webové aplikace dodá Objednatel Zhotoviteli před zahájením vlastního testování.
- vnitřní penetrační testy v provozním prostředí a běžném provozu vnitřní LAN sítě Objednatele.
Testy může Zhotovitel provádět on-site nebo rovněž prostřednictvím instalované síťové sondy, pokud takovou vlastní / provozuje.

4.3. Složení penetračních testů

Penetrační testy se budou skládat z:

- testů k získání informací, identifikace funkčních systémů;
- všeobecných testů zranitelnosti;
- testů týkajících se charakteristiky infrastruktury systému;
- testů existence backdoors;
- testů autentizace a schémat pro kontrolu přístupu;
- kontroly operačních systémů;
- testů aplikačních chyb a vad v systému;
- testů nedostatečného provozního zabezpečení;
- testování slabých míst zahrnující body selhání, s cílem způsobit odmítnutí služeb webových aplikací;
- odposlech komunikace se systémem;
- odchytení a přesměrování této komunikace;
- zneužití odchytených informací a komunikace směrem k aplikačním službám (serverům);
- sociálních útoků na uživatele systému prostřednictvím odchytených informací;
- testů přístupu přes wi-fi síť Objednatele.

Penetračním testováním prověří Zhotovitel celkovou kvalitu a odolnost nasazených bezpečnostních opatření. Jeho součástí bude nejen síťové skenování, ale i vyhodnocení konfigurace všech relevantních systémů.

Povinností Zhotovitele bude zajistit, aby v důsledku testování nedošlo k destruktivním dopadům.

Součástí požadovaného rozsahu testů není eskalace privilegií.

4.4. Postup testování

Testování bude Zhotovitel provádět v následujících fázích:

- Identifikace cíle;
- Identifikace aktivních služeb;
- Identifikace zranitelností;
- Získání přístupu;
- Eskalace privilegií a ovládnutí cíle;
- Reakce na testy.

V případě potřeby bude Zhotovitel oprávněn požádat Objednatele o individualizaci postupu testování v závislosti na typu webové aplikace, popřípadě IT infrastruktury.

Pro testování Zhotovitel využije především následující metodiky a doporučení týkající se bezpečnosti informačních systémů. Metodiky mohou být interně přizpůsobeny:

- Doporučení OWASP (Open Web Application Security Project), která se zaměřují na pomoc organizacím při identifikaci bezpečnostních hrozeb webových aplikací;
- Standard OSSTMM (Open Source Security Testing Methodology Manual) – metodologie pro testování bezpečnosti;
- Doporučení organizace IETF (Internet Engineering Task Force) – organizace vydávající RFCs tzv. standardy internetu;
- Doporučení organizace NIST (např. NIST SP 800-44 Guidelines on Securing Public Web Servers);
- Common Criteria (ISO/IEC 15408) – standard pro hodnocení úrovně bezpečnosti systémů;
- Materiály a doporučení ISACA (Information Systems Audit and Control Association) určené certifikovaným auditorům informačního systému (CISA);

Normy pro řízení bezpečnosti IS/ICT, řízení kvality projektu a provádění auditů:

- normy řady ISO/IEC 27000 pro oblast řízení bezpečnosti informačních systémů;
- BS 7799-3 Směrnice pro řízení rizik souvisejících s informační bezpečností;
- ČSN EN ISO 19011:2002 – Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu;
- ČSN ISO 10006 – Management jakosti – Směrnice jakosti v managementu projektu.

4.5. Počty testů

Celkem provede Zhotovitel 3 soubory testů:

- vstupní penetrační test (před zahájením implementace nástrojů pořízených projektem),
- výstupní penetrační test (před ukončením realizace projektu) a
- test zranitelnosti (před ukončením realizace projektu).

4.6. Prezentace výstupů testů

Všechny identifikované zranitelnosti Zhotovitel roztřídí do následující struktury:

- a) **dle hodnocení/kategorizace zranitelnosti** – veškeré nalezené problémy a zranitelnosti jsou rozděleny do pěti kategorií podle závažnosti:

C kriticky závažná chyba (**KRITICKÁ**) – CRITICAL

Jako kritické chyby jsou označeny nedostatky, které byly při testech zneužity a vedly (mohou vést) k přímé kompromitaci testovaného systému.

H závažné chyby (**VYSOKÁ**) – HIGH

Jako závažné klasifikujeme chyby, které bezprostředně umožňují kompromitaci systému, či jeho nedostupnost. U těchto chyb existuje velmi vysoká pravděpodobnost zneužití. Jejich okamžitá náprava bude nutná.

M středně závažné chyby (**STŘEDNÍ**) – MEDIUM

Do této kategorie spadají chyby, jejichž využití k potenciálnímu útoku na informační systém je technologicky náročnější na realizaci, nebo které umožňují průnik do systému pouze v případě splnění několika určitých navzájem souvisejících podmínek. Jejich závažnost nelze podceňovat s ohledem na potenciálně hrozící zneužití.

L méně závažné chyby (**NÍZKÁ**) – LOW

Tato kategorie zahrnuje méně závažné chyby, které napomáhají napadení systému. Např. poskytují potenciálnímu útočníkovi informace, jež lze uplatnit v rámci útoku



na informační systém – organizace o svém informačním systému prozrazuje více, než je nezbytně nutné. Ve většině případů se jedná pouze o konfigurační opomenutí apod.

I (INFORMATIVNÍ) – **INFO**

Informativní kategorie označuje vše, co lze zjistit o systémech a sítích, aniž by bylo možné jakýmkoliv způsobem zabránit úniku těchto informací. Tyto údaje nejsou většinou příliš důležité pro vedení vlastního útoku, ale mnohdy mohou napomoci útočníkovi při dokreslení či doplnění celkového obrazu o cíli potenciálního napadení.

- b) **dle klasifikace dle schopností útočníka** (skills, neboli schopnosti útočníka) je klasifikace, která popisuje nároky kladené na schopnosti a znalosti útočníka pro realizaci daného útoku:



Velmi znalí a zkušení útočníci, kteří k útokům používají úzce specializované a sofistikované nástroje. Jedná se o přesně cílené útoky.



Středně obtížná náročnost s využitím automatizovaných nástrojů. Technicky zdatní útočníci, kteří s větší mírou využívají manuální metody útoku, případně převzaté skripty.



Pro identifikaci a případné zneužití zranitelnosti postačují základní znalosti a schopnosti uživatele – útočníka. Ke zneužití může dojít také neúmyslnou chybou nebo náhodným jednáním.

Pro všechny zranitelnosti Zhotovitel uvede:

- a) **zjištění** – popis zranitelného místa/nálezu včetně popisu kde a jakým způsobem byla zranitelnost identifikována.
- b) **riziko** – popis rizik plynoucích z možného zneužití zranitelného místa včetně:
- možných scénářů zneužití (kdo a za jakých podmínek může zranitelnost zneužít a jaké jsou možné dopady tohoto zneužití),
 - posouzení dopadu rizika jednak na produkční prostředí a fungování Objednatele a jednak na možné legislativní a finanční postihy,
 - určení zdaje riziko akceptovatelné nebo ne.

5. Závěrečné zhodnocení – viz Ad. Kap. III

5.1. Předmět Zhodnocení

Zhodnocení bude obsahovat konkrétní vyhodnocení:

- a) zda současné digitální prostředí městského úřadu Telč splňuje požadavky na zajištění kybernetické bezpečnosti, a to:
- aktuálně platné, tzn. jak je shrnul výstupu části 1: Analýza rizik a další dokumentace systému řízení bezpečnosti informací projektu (konkrétně ve výstupu analýzy závazných povinností pro výkon činností objednatel z pohledu kybernetické bezpečnosti), tak
 - reálně očekávatelné v důsledku probíhající harmonizace nových směrnic (včetně NIS2) a nařízení Evropské unie, do právního rámce ČR, uvedené v předchozí = 1 části.
- b) jak projekt (tj. všech 10 částí) skutečně zvýšil kybernetickou bezpečnost Objednatele, tj.:
- zda realizace projektu zajistila zvýšení kybernetické odolnosti žadatelem definovaných informačních systémů na povinnou úroveň
 - do jaké zvýšil kybernetickou bezpečnost ostatních informačních aktiv Objednatele.

5.2. Požadovaná struktura Zhodnocení

5.2.1. Zjištění

Uvedená zjištění zpracuje Zhotovitel formou strukturovaného přehledu všech konkrétních zjištění souvisejících s jednotlivými zkoumanými oblastmi, a souhrn výstupů všech

provedených testů. Konkrétně se jedná o následující informace o stavu technické bezpečnosti prověřovaného systému a IT infrastruktury Objednatele:

- cíl a rozsah testu;
- popis předmětu testu;
- stanovení stupnice a metodiky hodnocení – kategorizace zjištěných zranitelností a jejich přehledné značení v rámci dokumentu;
- postup provedení testu včetně nástrojů a technik použitých v jednotlivých fázích;
- popis zjištění z jednotlivých fází testu;
- závěrečné zhodnocení provedení testu a hodnocení aktuálně dosažené úrovně bezpečnosti testovaných aplikací.
- popis specifikace případně zjištěných nalezených zranitelností (nedostatků aktuálního stavu kybernetické bezpečnosti Objednatele), každá v členění uvedeném níže;
- doporučení pro odstranění nebo alespoň snížení identifikovaných slabín a zranitelných míst;

5.2.2. Doporučení

Tato doporučení zpracuje Zhotovitel na základě posouzení přijatelnosti identifikovaných akceptovatelných rizik, tj. porovnání reálných nákladů na opatření vedoucí k snížení finančních dopadů identifikovaných rizik, formou konkrétních doporučení na odstranění nalezených nedostatků, případně návrhy na zvýšení bezpečnosti stávajících bezpečnostních mechanismů a opatření. Doporučení se mohou týkat procesních změn, konfigurace zařízení (hardening systémů), návrhu nových bezpečnostních mechanismů pro zvýšení stávající úrovně bezpečnosti, doporučení pro uživatelská PC pro zvýšení bezpečnosti atd.

6. **Ad část manažerské shrnutí**

V této části závěrečné zprávy Zhotovitel pro účely managementu Objednatele maximálně stručně, jednoznačně a srozumitelně:

- shrne informace o průběhu Auditů,
- zrekapituluje klíčové závěry hodnocení bezpečnostních zjištění,
- uvede konkrétní návrhy, která Zhotovitel auditu doporučuje realizovat pro odstranění zjištěných nedostatků a pro posílení celkového zabezpečení. (podrobně je konkrétní specifikace těchto opatření popsána v Kapitole 1).

7. **Ad část přílohy**

V této část hodnotící zprávy Zhotovitel uvede veškeré přílohy, tj.: výstupy z použitých nástrojů, printscreeny, důkazy apod.

Součástí této kapitoly bude i posudek nezávislého auditora, který odpoví na klíčové otázky týkající se realizace opatření a jejich dopadu na kybernetickou bezpečnost,

8. **Všechny výstupy a procesy zjišťování a hodnocení**

V rámci hodnocení bude zohledněna analýza výchozího stavu dle dokumentace poskytnuté Objednatelem. Finální audit bude zaměřen na ověření naplnění požadavků na kybernetickou bezpečnost prostřednictvím certifikovaného auditora, který vystaví posudek v souladu s požadavky Národního plánu obnovy.