# Smlouva o dílo

(dále jen „***Smlouva***“)
Číslo smlouvy objednatele: **2021002038**
Číslo smlouvy zhotovitele: **2021-TS_SM ČB-10**

**Statutární město České Budějovice**
se sídlem nám. Přemysla Otakara II. 1/1, 370 92 České Budějovice
IČO: 00244732
DIČ: CZ00244732
zastoupené Ing. Viktorem Vojtkem, Ph.D., náměstkem primátora statutárního města České Budějovice, na základě plné moci
(dále jen „***Objednatel***“)

**-a-**

**TOTAL SERVICE a.s.**
se sídlem U Uranie 954/18, Holešovice, 170 00 Praha 7
IČO: 256 18 067
DIČ: CZ25618067
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 23580
zastoupená Jiřím Chovancem, členem představenstva

(dále jen „***Zhotovite***l“)
(dále společně též jako „***Smluvní strany***“ nebo též samostatně jako „***Strana***“)

uzavřeli tuto **Smlouvu o dílo** v souladu s ustanovením § 2586 a násl. zákona č. 89/2012 Sb., občanského zákoníku, v platném a účinném znění

**Smluvní strany, vědomy si svých závazků v této Smlouvě obsažených a s úmyslem být touto Smlouvou vázány, dohodly se na následujícím znění Smlouvy:**

## 1. PŘEDMĚT SMLOUVY

1.1. Zhotovitel se touto Smlouvou zavazuje provést pro Objednatele dílo, spočívající v **„Penetračním testování IT infrastruktury MMČB“** (dále jen ***„Dílo“***), složené z těchto částí:

a. Externí penetrační testy
b. Penetrační testy webové aplikace
c. Penetrační testy WiFi sítě
d. Testy sociálním inženýrstvím
e. Vypracování závěrečné zprávy

1.2. Podrobná specifikace Díla je obsažena v Příloha č.1 této Smlouvy.

## 2. MÍSTO A TERMÍN PROVEDENÍ DÍLA

2.1. Místem provedení Díla, tj. místem provádění testů dle čl. 1., je sídlo Objednatele a je-li to technicky proveditelné a Objednatel s tím vysloví souhlas, mohou být tyto testy prováděny též vzdáleně ze sídla Zhotovitele, popř. jiného místa při zajištění dostatečného zabezpečení takového přístupu. Místem pro předání výstupů Díla dle Přílohy č. 1 je vždy sídlo Objednatele.

2.2. Harmonogram provedení a termín dodání Díla je stanoven v Příloze č. 2 této Smlouvy v rámci sjednaného harmonogramu plnění, popřípadě je určen pevným datem.

## 3. PŘEDÁNÍ A PŘEVZETÍ DÍLA

3.1. Předání a převzetí Díla proběhne prostřednictvím akceptační procedury, která zahrnuje porovnání skutečného provedení Díla se specifikací Díla uvedenou v Příloze č. 1 této Smlouvy a dle Přílohy č. 4 této Smlouvy.

3.2. Při převzetí Díla se Objednatel i Zhotovitel zavazují podepsat příslušný Předávací protokol, t.j. Potvrzení o předání a přijetí (převzetí) Díla. V případě, že Objednatel odmítne Dílo převzít bez výhrad, bude sepsán předávací protokol s uvedením podrobné specifikace výhrad.

3.3. Objednatel nemá zájem na částečném plnění Díla.

## 4. CENA – ODMĚNA A PLATEBNÍ PODMÍNKY

4.1. Cena za provedení Díla byla dohodou Smluvních stran stanovena na částku ve výši **165.000,- Kč** (slovy jedno sto šedesát pět tisíc korun českých) bez DPH. Ke sjednané ceně bude připočtena daň z přidané hodnoty ve výši stanovené právními předpisy platnými v době uskutečnění zdanitelného plnění.

4.2. Sjednaná celková cena je nejvýše přípustná a zahrnuje v sobě veškeré náklady, které má Zhotovitel se splněním závazků z této Smlouvy.

4.3. Objednatel se zavazuje cenu za provedení Díla dle předchozího článku zaplatit na účet Zhotovitele po úplné akceptaci Díla dle této Smlouvy, respektive po vypořádání všech výhrad. Cena je splatná na základě daňového dokladu – faktury vystavené Zhotovitelem po předání a akceptaci Díla bez výhrad.

4.4. Splatnost všech faktur činí 30 (třicet) dní ode dne jejich doručení druhé Smluvní straně povinné platit. Faktura se považuje za doručenou třetím dnem po jejím prokazatelném odeslání druhé Smluvní straně.

4.5. V případě prodlení Objednatele s úhradou faktury dle odst. 4.3 je Objednatel povinen zaplatit Zhotoviteli úrok z prodlení, který si Smluvní strany ujednávají ve výši 0,02 % z dlužné částky, a to za každý i započatý den prodlení.

## 5. UŽÍVÁNÍ DÍLA – POSKYTNUTÍ LICENCÍ

5.1. Objednatel nabývá dnem podpisu akceptačního protokolu oprávnění Dílo, ve smyslu AutZ (zákon č. 121/2000 Sb., autorský zákon, v platném a účinném znění), užít všemi způsoby uvedenými v ustanovení § 12 AutZ. Toto oprávnění Zhotovitel Objednateli poskytuje trvale, tzn. bez časového omezení.

5.2. Objednatel je oprávněn užívat Dílo ke všem způsobům uvedeným v autorském zákoně a za podmínek touto Smlouvou stanovených. Na základě dohody Smluvních stran je odměna za oprávnění k užití Díla zahrnuta v ceně za Dílo dle této smlouvy.

5.3. Objednatel nabývá vlastnické právo k hmotnému nosiči dat, na kterém je zaznamenáno Dílo dnem úplného zaplacení ceny – odměny podle této Smlouvy.

## 6. OPRÁVNĚNÉ OSOBY

6.1. Každá ze Smluvních stran jmenuje oprávněnou osobu či oprávněné osoby. Oprávněné osoby budou zastupovat Smluvní stranu ve smluvních a obchodních záležitostech souvisejících s plněním této Smlouvy.

6.2. Jména oprávněných osob jsou uvedena v **Příloze č. 3** této Smlouvy. Smluvní strany jsou oprávněny změnit oprávněné osoby, jsou však povinny na takovou změnu druhou Smluvní stranu bez zbytečného odkladu písemně upozornit.

## 7. OCHRANA INFORMACÍ

7.1. Smluvní strany jsou povinny zajistit utajení získaných důvěrných informací způsobem obvyklým pro utajování takových informací, není-li výslovně sjednáno jinak. Tato povinnost platí bez ohledu na ukončení účinnosti této Smlouvy. Strany mají právo požadovat navzájem doložení dostatečnosti utajení důvěrných informací. Strany jsou povinny zajistit utajení důvěrných informací i u svých

zaměstnanců, zástupců, jakož i jiných spolupracujících třetích stran, pokud jim takové informace byly poskytnuty.

7.2. Právo užívat, poskytovat a zpřístupnit důvěrné informace mají obě Strany pouze v rozsahu a za podmínek nezbytných pro řádné plnění práva a povinností vyplývajících z této Smlouvy.

7.3. Za důvěrné informace se bez ohledu na formu jejich zachycení považují veškeré informace, které nebyly některou ze Stran označeny jako veřejné a které se týkají této Smlouvy a jejího plnění (zejména informace o právech a povinnostech Stran jakož i informace o cenách, informace o zabezpečení IT infrastruktury Objednatele a jeho slabých místech, apod.), které se týkají některé ze Stran (zejména obchodní tajemství, informace o jejich činnosti, struktuře, hospodářských výsledcích, know-how) anebo informace pro nakládání, s nimiž je stanoven právními předpisy zvláštní režim utajení (zejména hospodářské tajemství, státní tajemství, bankovní tajemství, služební tajemství). Dále se považují za důvěrné informace takové informace, které jsou jako důvěrné výslovně některou ze Stran označeny.

7.4. Za důvěrné informace se v žádném případě nepovažují informace, které se staly veřejně přístupnými, pokud se tak nestalo porušením povinnosti jejich ochrany, dále informace získané na základě postupu nezávislého na této Smlouvě nebo druhé Straně, pokud je Strana, která informace získala, schopna tuto skutečnost doložit, a konečně informace poskytnuté třetí osobou, která takové informace nezískala porušením povinnosti jejich ochrany. Za důvěrné se rovněž nikdy nepovažují informace, které mohou být uveřejněny či poskytnuty v souladu s ujednáním Smluvních stran dle čl. 11.3, resp. na základě tam uvedených právních a jiných předpisů.

7.5. Žádné ustanovení této Smlouvy přitom nebrání nebo neomezuje Zhotovitele ve zveřejnění nebo obchodním využití jakékoliv technické znalosti, dovednosti nebo zkušenosti obecné povahy, kterou získal při plnění této Smlouvy.

7.6. Zhotovitel je oprávněn užít informaci o existenci smluvního vztahu mezi účastníky této Smlouvy pro účely svého marketingu a reklamy. Ustanovení této Smlouvy o ochraně důvěrných informací tím není dotčeno.

7.7. Zachování důvěrnosti a ochrany informací získaných během testování bude platné i po ukončení prací, a to po dobu minimálně 8 (osmi) let.

## 8. SOUČINNOST A VZÁJEMNÁ KOMUNIKACE

8.1. Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků. Smluvní strany jsou povinny informovat druhou Smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této Smlouvy. Smluvní strany jsou povinny plnit své závazky vyplývající z této Smlouvy tak, aby nedocházelo k prodlení s plněním jednotlivých termínů a s prodlením splatnosti jednotlivých peněžních závazků.

8.2. Veškerá komunikace mezi Smluvními stranami bude probíhat prostřednictvím oprávněných osob, statutárních orgánů Smluvních stran, popř. jimi pověřenými pracovníky.

## 9. NÁHRADA ŠKODY A SANKCE

9.1. Zhotovitel nese odpovědnost za způsobenou škodu v rámci platných právních předpisů a této Smlouvy. Obě strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.

9.2. Žádná ze stran neodpovídá za škodu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé Strany. Žádná ze Smluvních stran není odpovědná za prodlení způsobené prodlením s plněním závazků druhé Smluvní strany.

9.3. Smluvní strany se zavazují upozornit druhou Smluvní stranu bez zbytečného odkladu na vzniklé okolnosti bránící řádnému plnění této Smlouvy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání okolností bránících řádnému plnění této Smlouvy.

9.4. Při prodlení s provedením Díla a jeho odevzdáním Objednateli v rozporu s termínem dodání finální zprávy uvedeným v Příloze č. 2 této Smlouvy, se Zhotovitel zavazuje Objednateli uhradit smluvní pokutu ve výši 0,2 % z celkové ceny Díla bez DPH (dle čl. 4 této Smlouvy), a to za každý i započatý den prodlení.

9.5. Každá ze Smluvních stran je oprávněna požadovat v plné výši náhradu škody i v případě, že se jedná o porušení povinnosti přesto, že uplatnila za dané porušení smluvní pokutu.

9.6. Smluvní pokuta dle této Smlouvy je splatná do 30 (třiceti) pracovních dnů od doručení faktury druhé Smluvní straně.

9.7. Případná náhrada škody bude zaplacena v českých korunách.

## 10. PLATNOST A ÚČINNOST SMLOUVY

10.1. Tato Smlouva nabývá účinnosti dnem jejího dnem jejího uveřejnění v centrálním registru smluv.

10.2. Objednatel je oprávněn krom případů dle příslušných ustanovení občanského zákoníku odstoupit od Smlouvy v případě, že Zhotovitel je v prodlení s dodáním Díla proti časovému harmonogramu, uvedenému v Příloze č. 2 této Smlouvy, déle než 30 (třicet) dnů a nesjedná nápravu ani do 15 (patnácti) dnů od doručení písemného oznámení Objednatele o takovém prodlení.

10.3. Zhotovitel je oprávněn krom případů dle příslušných ustanovení občanského zákoníku odstoupit od Smlouvy též v případě, kdy je Objednatel v prodlení s placením faktur vystavených Zhotovitelem, a toto prodlení trvá po dobu delší než 15 (patnáct) dní po písemném upozornění a dále je oprávněn odstoupit od Smlouvy též v případě, že Objednatel je v prodlení s plněním jiných svých závazků podle této Smlouvy déle než 30 (třicet) dní a nezjedná nápravu ani do 15 (patnácti) dnů od doručení písemného oznámení Zhotovitele o takovém prodlení.

## 11. ZÁVĚREČNÁ USTANOVENÍ

11.1. Tato Smlouva představuje úplnou dohodu Smluvních stran o předmětu této Smlouvy. Tuto Smlouvu je možné měnit pouze písemnou dohodou Smluvních stran, a to ve formě vzestupně číslovaných dodatků této Smlouvy, podepsaných oprávněnými zástupci obou Smluvních stran.

11.2. Zhotovitel vylučuje přijetí návrhu na uzavření Smlouvy nebo dohody nebo jakéhokoliv ujednání, souvisejícího s touto Smlouvou, s jakýmkoli dodatkem či odchylkou; odpověď na nabídku s dodatkem či odchylkou se nepovažuje za přijetí nabídky ale za nový návrh, který musí být znovu akceptován druhou Smluvní stranou.

11.3. Zhotovitel bere na vědomí, že na tuto Smlouvu se vztahují povinnosti uveřejnění dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, v platném a účinném znění, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), v platném znění. Smluvní strany si tímto ujednávají, že uveřejnění dle tohoto zákona zajistí Objednatel způsobem, v rozsahu a ve lhůtách z něho vyplývajících. O provedeném uveřejnění Objednatel Zhotovitele informuje poté, co obdrží ze strany správce registru smluv potvrzení o provedeném uveřejnění. Smluvní strany po dohodě souhlasí rovněž s tím, že úplné znění této Smlouvy včetně všech jejích Příloh a dalších součástí může být bez omezení zveřejněno i na oficiálních webových stránkách města České Budějovice (www.c-budejovice.cz). Zhotovitel bere dále na vědomí, že Objednatel je povinen či oprávněn tuto Smlouvu, jakož i jiné skutečnosti z ní nebo z jejího naplňování vyplývající, uveřejnit či poskytnout třetím osobám, pokud takový postup vyplývá z jiných právních předpisů. Pro účely uveřejňování či poskytování dle předchozích vět Smluvní strany současně shodně prohlašují, že žádnou část této Smlouvy nepovažují za své obchodní tajemství bránící jejímu uveřejnění či poskytnutí. Ujednání dle tohoto odstavce se vztahují i na všechny případné dodatky k této Smlouvě, jejichž prostřednictvím je tato Smlouva měněna či ukončována.

11.4. Vyhrazená změna závazku:

11.4.1. Objednatel si v souladu s § 100 odst. 2 zákon č. 134/2016 Sb. (dále jen „ZZVZ“) vyhrazuje v případě naplnění některé z podmínek pro odstoupení Smluvní strany stanovené v čl. 10 této Smlouvy změnu Zhotovitele v průběhu plnění veřejné zakázky a jeho nahrazení účastníkem zadávacího řízení, který se dle výsledku hodnocení umístil druhý v pořadí, a to za cenových podmínek obsažených v nabídce tohoto v pořadí druhého účastníka zadávacího řízení v souladu se závazným návrhem Smlouvy dle zadávací dokumentace.

11.4.2. Pokud účastník zadávacího řízení, který se dle výsledků hodnocení umístil druhý v pořadí, odmítne poskytovat plnění namísto původně vybraného Zhotovitele za podmínek uvedených v předchozím odstavci, je Objednatel oprávněn obrátit se na účastníka zadávacího řízení, který se umístil jako třetí v pořadí.

11.5. Nedílnou součást Smlouvy tvoří tyto přílohy:

Příloha č. 1 Specifikace Díla

Příloha č. 2 Termín plnění a harmonogram provedení prací

Příloha č. 3 Oprávněné osoby

Příloha č. 4 Nabídka Zhotovitele

11.6. Tato Smlouva je Smluvními stranami uzavírána výlučně v elektronické podobě, a to připojením uznávaného elektronického podpisu zástupců Smluvních stran.

**Strany prohlašují, že si tuto Smlouvu přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují svoje podpisy.**

| **Zhotovitel** | **Objednatel** |
|---|---|
| V Praze dne 26. listopadu 2021 | V Českých Budějovicích dne __.__._____ |
| Jiří Chovanec<br>Digitálně podepsal Jiří Chovanec<br>Datum: 2021.12.20 13:19:25 +01'00' | |
| ..... | ..... |
| **TOTAL SERVICE a.s.**<br>Jiří Chovanec<br>člen představenstva | **Statutární město České Budějovice**<br>Ing. Viktor Vojtko, Ph.D.<br>náměstek primátora |

# Příloha č.1
## Specifikace Díla

**PENETRAČNÍ TESTOVÁNÍ IT INFRASTRUKTURY MMČB**

## 1. Externí penetrační testy

Provedení externích penetračních testů s cílem zjistit, jak snadno identifikovatelný cíl ICT infrastruktura organizace představuje, jaké informace lze získat o zvenčí dostupných komponentách, jak detekovat zranitelnosti, které mohou být zneužity k získání neautorizovaného přístupu k citlivým systémovým zdrojům, a navrhnout doporučení k jejich odstranění. Testy musí být vedeny z prostředí Zhotovitele prostřednictvím Internetu.

Předpokládáme, že testy zahrnou následující činnosti:

### Identifikace cíle

Sběr z internetu dostupných informací o IT prostředí Objednatele (evidenční databáze, DNS, trasování, odezvy apod.).

### Identifikace aktivních služeb

Skenování portů a identifikace otevřených portů

### Identifikace zranitelností

Zjištění existujících zranitelností a výběr těch, které mohou být potencionálně zneužity ke kompromitaci prostředí Objednatele

### Získání přístupu

S využitím nalezených zranitelností a dalších informací zjištěných v předchozích fázích se pokusit o průnik do aplikace/systému, případně získat citlivé informace (např. uživatelská hesla).

### Eskalace privilegií a ovládnutí cíle

Pokusit se o získání plné kontroly nad kompromitovanými aplikacemi/systémy (např. získání práva uživatele administrátor), identifikovat možnosti instalace dalších aplikací (např. pro vzdálené ovládání cíle), identifikovat možnosti využití aplikace k útoku a průnikům do dalších aplikací Objednatele.

### Reakce na testy

Analyzovat případné reakce ochranných nástrojů Objednatele směřující proti prováděným testům (např. reakce IPS, administrátorů apod.).

### Rozsah prostředí

Testy budou prováděny nad IT technikou a systémy v majetku statutárního města České Budějovice, umístěnými v budovách Magistrátu města České Budějovice, Městské policie ČB a Sportovních zařízení města České Budějovice.

### Podmínky testování

Veškeré testy budou prováděny bez destruktivních zásahů tzn., že útok končí kompromitací systému, neprovádějí se žádné změny, které by poškodily nebo jakkoli ovlivnily informační systém MMČB.

## 2. Penetrační testy webových aplikací Objednatele

Penetrační testy prověří aplikace z pohledu spolehlivosti, zajištění integrity a důvěrnosti dat. Testy musí být zaměřeny také na identifikaci bezpečnostních slabin.

V rámci testů budou otestovány aplikace **www.c-budejovice.cz**, **www.inbudejovice.cz,** **mpolicie.c-budejovice.cz**.

Předpokládáme, že penetrační testy webových aplikací zahrnou následující kroky:

- kontrola nastavení bezpečné komunikace (např. pomocí https, ssl);

- bezpečnost kritických datových toků;
- chyby aplikací (výpočty, náhodné chyby, ztráta dat);
- možnost zneužití aplikací neautorizovaným způsobem, kontrola hodnot při zadání uživatelem;
- stabilita aplikací;
- posouzení bezpečnostní úrovně;
- pokus o získání přihlašovacích údajů registrovaného uživatele;
- náchylnost na aplikační zranitelnosti definované v rámci projektu OWASP;
- bezpečnost technologií, na kterých jsou systémy postaveny (operační systémy, webové, aplikační a databázové servery) a bezpečnost jejich integrace do zbývající infrastruktury;
- možnosti zneužití technologií dostupných v aplikaci útočníkem a otestování hrozby útoku na účty/relace legitimních klientů.

Testy musí být provedeny na úrovni anonymního uživatele. Jedná se o prověření aplikace bez znalosti prostředí a představuje tak simulaci napadení webové aplikace útočníkem, který má k dispozici pouze veřejně dostupné informace. Cílem testů je detekovat zranitelnosti, které mohou být zneužity k získání neautorizovaného přístupu k citlivým informacím a systémovým zdrojům.

Součástí testů je ohodnocení možností anonymního útočníka vzhledem k získání neautorizovaného přístupu k systému – zde očekáváme, že aplikace budou testovány na možnosti unesení relace, útoky MITM (Man In The Middle), zcizení autentizačních údajů apod.

# 3. Bezpečnostní audit WiFi sítě

Cílem penetračních testů WiFi technologií simulace útoku na přístup do vnitřní sítě organizace prostřednictvím bezdrátového signálu WiFi sítí. Po získání přístupu musí být prověřena kvalita filtrování provozu mezi síťovým segmentem WiFi klientů a zbytkem interní sítě.

Součástí testů bude také analýza konfigurace připojení k bezdrátové síti na straně klientských zařízení. Výstupem testu bude přehled a zmapování provozovaných WiFi sítí a seznam bezpečnostních nálezů s následným možným dopadem na vnitřní síť Objednatele.

Test má za cíl analyzovat zabezpečení WiFi sítě. Součástí bude provedení útoků s cílem získání přístupu a následně zmapování prostupů ze segmentu WiFi klientů do segmentu vnitřní sítě společnosti.

Cílem je co nejvěrněji simulovat postup případného útočníka. Veškeré útoky mohou být provedeny nejen za pomocí volně dostupných nástrojů a aplikací, ale i pomocí proprietárních nástrojů Zhotovitele.

# 4. Testy sociálním inženýrstvím

Cílem testu je prověřit úroveň bezpečnostního povědomí zaměstnanců – uživatelů informačního systému Objednatele a jejich odolnost vůči scénářům útoků, které simulují pravděpodobnou činnost skutečného útočníka, který by se mohl v praxi pokusit tímto způsobem napadnout informační systém společnosti.

Předpokládáme využití nejrůznějších metod, kterými se útočník pokusí, zpravidla pomocí falešné identity, různých forem nátlaku a s využitím komunikačních prostředků (telefon, e-mail), přinutit uživatele sdělit určité citlivé informace nebo vykonat určitou činnost, která realizuje nebo usnadňuje útok na samotný informační systém organizace.

Při realizaci testování metodami sociálního inženýrství bude Zhotovitel vycházet zejména z údajů dostupných na webových stránkách Objednatele nebo jinde na internetu (získání kontaktů na konkrétní zaměstnance a hledání záminek k útokům). Test tedy bude veden tzv. black-box přístupem.

## 4.1. E-mailový test

Cílem tohoto testu bude Zhotovitelem kontrolovaný útok e-mailové adresy zaměstnanců získané na webových stránkách Objednatele, jinde na internetu, odhadnuté podle jmen zaměstnanců získaných jiným způsobem apod. Na tyto e-mailové adresy pak budou směřovány útoky dle různých scénářů (záminek, ať již spojených s činností společnosti nebo s jinými zjištěnými skutečnostmi pracovní či nepracovní povahy), jejichž cílem bude přinutit zaměstnance spustit testovací kód (soubor) simulující malware. Tento kód může být vložen přímo v e-mailu nebo může být umístěn na internetu a stažen do počítače „oběti“ prostřednictvím podstrčeného odkazu.

Test bude považován (z pohledu „útočníka“) za úspěšný, pokud testovaný zaměstnanec kód spustí, což bude indikováno v logu monitorovacího serveru.

V rámci testu přepokládáme otestování nejméně 100 náhodně vybraných zaměstnanců Objednatele (zaměstnanci zařazení do Magistrátu města České Budějovice a administrativní pracovníci Městské policie České Budějovice).

### 4.2. Telefonický test

Cílem tohoto testu budou telefonní čísla zaměstnanců Objednatele získaná na webových stránkách Objednatele nebo jinde na internetu či jiným způsobem (např. telefonickým oslovením na obecné telefonní číslo apod.). Na tato zjištěná telefonní čísla budou směřovány útoky dle různých scénářů, jejichž cílem bude přinutit zaměstnance vyzradit nějakou citlivou informaci (např. svoje přihlašovací jméno a heslo) nebo spustit testovací kód (soubor) simulující malware podobně jako u e-mailového testu.

Test bude považován (z pohledu „útočníka“) za úspěšný, pokud testovaný zaměstnanec vyzradí požadovanou informaci nebo spustí podstrčený kód. Validita zjištěných informací bude následně dle možností ověřována a budou pořizovány důkazy formou screenshotů apod.

V rámci testu bude osloveno nejméně 20 Zhotovitelem náhodně zvolených zaměstnanců Objednatele (zaměstnanci zařazení do Magistrátu města České Budějovice a administrativní pracovníci Městské policie České Budějovice).

### 4.3. Fyzický test

Cílem tohoto testu budou informace o cílových lokalitách zjistitelné na webu Objednatele, jinde na internetu, případně fyzickou obhlídkou těchto lokalit před samotným simulovaným útokem. Na základě těchto zjištěných informací budou následně učiněny pokusy neautorizovaných osob o průnik do vnitřních prostor Objednatele.

Test bude (z pohledu „útočníka“) považován za úspěšný, pokud neautorizované osoby úspěšně proniknou do vnitřního perimetru dané lokality a získají (zneužitelný) přístup k prostředkům informačního systému, přístup k citlivým informacím Objednatele apod. Tyto skutečnosti i průběh testu bude dle možností dokumentován fotograficky nebo pomocí video nahrávek, případně budou pořizovány jiné formy důkazů.

O celém testu bude podrobně (a v průběhu testu i operativně o postupu) informován vedoucí OICT, který bude v případě odhalení průniku nebo jiné eskalované situace kontaktován a který případně rozkryje prováděný test cílovým zaměstnancům.

Pokud tester nalezne v budovách Magistrátu města České Budějovice veřejně dostupný LAN port, umožňující přístup do vnitřní sítě MMČB, může k němu připojit zařízení tak, že bude schopné zachytávat interní komunikaci. Fyzické připojení jakéhokoliv zařízení testera do vnitřní sítě MMČB (na nalezeném dostupném portu) podléhá předchozímu telefonickému oznámení vedoucímu OICT (pouze jemu).

Fyzický test bude proveden ve spojení s testy WiFi.

## 5. Obsah a struktura závěrečné zprávy z testů

Výstupem penetračních testů bude závěrečná zpráva o stavu technické bezpečnosti prověřovaných aplikací, která bude obsahovat část manažerského shrnutí (může být i samostatným dokumentem) a detailní zprávu o provedeném testování. Výstupy budou předány v papírovém originále a rovněž elektronicky v podobě zašifrovaného archivu, uloženého na DVD či flash disku, spolu s výstupy z použitých testovacích nástrojů a případnými doplňujícími informacemi k testům (např. screenshoty z průběhu testů).

Zpráva bude vypracována v českém jazyce.

**Manažerské shrnutí**

Pro vedení města bude vypracována speciální hodnotící zpráva s cílem podchytit a stručně a srozumitelně popsat zjištěné výsledky testování a analýz. Cílem manažerského shrnutí je podat stručné informace o průběhu projektu, ohodnotit bezpečnost jak celého systému aplikací, tak i jednotlivých zkoumaných oblastí, a popsat nejdůležitější doporučovaná bezpečnostní opatření, která budou podrobně popsána v detailní zprávě.

**Detailní zpráva**

Obsahem detailní zprávy budou konkrétní zjištění související s jednotlivými zkoumanými oblastmi. Detailní zpráva bude zahrnovat zejména následující informace:

- Cíl a rozsah projektu.
- Popis předmětu projektu.

- Stanovení stupnice a metodiky hodnocení – kategorizace zjištěných zranitelností a jejich přehledné značení v rámci dokumentu.
- Detailní postup provedených testů včetně nástrojů a technik použitých v jednotlivých fázích.
- Popis zjištění z jednotlivých fází testů.
- Popis nalezených zranitelnosti, každá v členění uvedeném níže.
- Doporučení pro odstranění identifikovaných slabin a zranitelných míst.
- Závěrečné zhodnocení provedeného testu a hodnocení aktuálně dosažené úrovně bezpečnosti testovaných aplikací, resp. prostředí.

Všechny identifikované zranitelnosti budou popsány v následující struktuře, pokud nebude mezi Objednatelem a Zhotovitelem dohodnuto jinak:

1. **Hodnocení/kategorizace zranitelnosti** – veškeré nalezené problémy a zranitelnosti budou rozděleny nejméně do čtyř kategorií podle závažnosti.

| | |
|---|---|
| **Závažné chyby (VYSOKÁ/HIGH)** | Jako závažné budou klasifikovány chyby, které bezprostředně umožňují kompromitaci systému, či jeho nedostupnost. Jejich okamžitá náprava je nutná. |
| **Středně závažné chyby (STŘEDNÍ/MEDIUM)** | Do této kategorie spadají chyby, jejichž využití k potenciálnímu útoku na IS 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. |
| **Méně závažné chyby (NÍZKÁ/LOW)** | Chyby, které napomáhají napadení systému, např. poskytují potenciálnímu útočníkovi informace, jež lze uplatnit v rámci útoku na IS – organizace o svém IS prozrazuje více, než je nezbytně nutné. Ve většině případů se jedná pouze o konfigurační opomenutí apod. |
| **Informativní nálezy (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. |

2. **Klasifikace dle pravděpodobnosti zneužití** – je klasifikace, která popisuje nároky kladené na schopnosti a znalosti útočníka, dostupnost nástrojů pro realizaci daného útoku a celkově proveditelnost a náročnost popsaného útoku.

| | |
|---|---|
| **VYSOKÁ/HIGH** | Pro identifikaci a případné zneužití zranitelnosti postačují základní znalosti a schopnosti uživatele – útočníka. Ke zneužití může dojít také neúmyslnou chybou nebo náhodným jednáním. Pravděpodobnost zneužití chyby je vysoká. |
| **STŘEDNÍ/MEDIUM** | Středně obtížná náročnost s využitím automatizovaných nástrojů. Technicky zdatní útočníci, kteří s větší mírou využívají manuální metody útoku, případně převzaté skripty. Pravděpodobnost zneužití chyby je středně vysoká. |
| **NÍZKÁ/LOW** | Velmi znalí a zkušení útočníci, kteří k útokům používají úzce specializované a sofistikované nástroje. Jedná se o přesně cílené útoky vyžadující hluboké znalosti nebo kombinaci několika nepravděpodobných scénářů. Pravděpodobnost zneužití chyby je nízká. |

3. **Klasifikace dle náročnosti odstranění zranitelnosti** – každá identifikovaná zranitelnost bude klasifikována také z pohledu odhadované náročnosti úpravy systému nebo zavedení jiného opatření pro snížení rizika nebo úplné odstranění zranitelnosti.

| | |
|---|---|
| **VYSOKÁ/HIGH** | Pro odstranění zranitelnosti klasifikované tímto stupněm se předpokládá nutnost rozsáhlejších, strukturálních změn v kódu aplikace nebo její kompletní |

| | |
|---|---|
| | přepracování, nasazení nových technologií na úrovni infrastruktury nebo rozsáhlé změny infrastruktury. |
| **STŘEDNÍ/MEDIUM** | Pro odstranění zranitelnosti klasifikované tímto stupněm bude potřeba udělat středně rozsáhlé změny v kódu aplikace, rozsáhlejší rekonfigurace serveru nebo související infrastruktury. |
| **NÍZKÁ/LOW** | Pro odstranění zranitelnosti klasifikované tímto stupněm se předpokládá implementace nápravných opatření v podobě úpravy konfiguračních parametrů aplikace nebo související infrastruktury. |

# Příloha č. 2
## Termíny plnění a harmonogram provedení prací

Harmonogram provedení prací:

Testování bude zahájeno v do T+14 dní.

Předpokládané ukončení je do T+20 dní.

Čas T je časem účinnosti Smlouvy. Termíny předpokládají součinnost klienta se zpřístupněním prostor a poskytnutí ethernet konektivity.

Dílčí termíny uvedené v harmonogramu jsou nezávazné a Zhotovitel je může se souhlasem Objednatele upravovat bez nutnosti uzavírání dodatku ke Smlouvě. Úpravy dle předchozí věty však nesmí mít vliv na termín dodání finální zprávy.

Termín dodání finální zprávy: do T+45 dní.

Termín pro dodání finální zprávy nesmí být delší, než 90 dnů od data účinnosti Smlouvy.

# Příloha č. 3
## Oprávněné osoby

Pro obchodní jednání:

za Zhotovitele TOTAL SERVICE a.s.
Jiří Quirsfeld

za Objednatele (Magistrát města České Budějovice)
Mgr. David Kříž, vedoucí OICT

Pro provádění Díla:

za Zhotovitele TOTAL SERVICE a.s.
Daniel Přívratský, Service Manager

za Objednatele (Magistrát města České Budějovice)
Mgr. David Kříž, vedoucí OICT
Bc. Filip Vrátný, Městská policie města ČB

# Příloha č. 4
## Nabídka Zhotovitele

# 1. Rozsah projektu – bezpečnostní test

Tento dokument tvoří zadání bezpečnostního testu definuje testovací metodiku a postupy včetně dohledu průběhu testu, zvládání mimořádných situací, výjimek a omezení, na které bude během testování brán zřetel. Dále slouží k oboustranné dohodě a potvrzení testu zranitelností.

Realizace testu bude probíhat s využitím automatizovaných nástrojů pro skenování zranitelností v ICT a OT technologiích a službách s následným manuálním ověřením, přičemž cílem je zmapování maximálního možného počtu potenciálních zranitelností a bezpečnostních slabin, které jsou důsledkem chybějících bezpečnostních záplat na známé zranitelnosti a/nebo nedostatečné konfigurace operačních systémů a aplikačního software.

Z důvodu citlivosti testování je potřebné zafixovat pravidla testu v tomto dokumentu takovým způsobem, aby test proběhl v předem definované formě a kvalitě, čímž se minimalizují případná rizika.

## 1. Základní informace o testu

### 1.1. Časový rámec testu

Detailní časový harmonogram bezpečnostního testu organizace MMČB bude upřesněn před zahájením testu.

### 1.2. Cíl a rozsah testů

Bezpečnostní test se bude skládat z

- Externího penetračního testu
- Externího penetračního testu webových aplikací www.c-budejovice.cz, www.inbudejovice.cz, mpolicie.c-budejovice.cz.
- Penetračního testu wifi sítě v prostorách MMČB
- Externího testu sociálním inženýrstvím zahrnující
    - Emailový test
    - Telefonický test
    - Fyzický test

Testované prostředí bude zahrnovat:

- Služby veřejně dostupné ze sítě Internet
- Prostory MMČB na adrese nám. Přemysla Otakara II. 1/1, 370 92 České Budějovice

Cílem bezpečnostního testu bude ověřit zda:

- lze získat neoprávněný přístup ke službám/datům/systémům,
- lze neoprávněně modifikovat/zničit data procházející komunikační infrastrukturou nebo zpracovávaná/uložená na systémech,
- lze proniknout bezpečnostním prvky,
- lze získat autentizační údaje,
- lze zneužít infrastrukturu k útokům na sítě a služby třetích stran a
- existují zranitelnosti, které mohou vést k předchozím bodům.

Testování zranitelností bude realizováno v uvedených oblastech vždy s využitím aktuálních dostupných databází zranitelností a nedostatků v implementaci nebo konfiguraci jednotlivých technologiích:

- definovaného IP rozsahu
- síťové infrastruktury
- bezpečnostního prvku
- HW serveru/pracovní stanice
- virtualizační platformy
- OS Microsoft Windows / OS Linux

Cílem prověrky bude odhalení případných bezpečnostní slabin a navrhnout účinná opatření k jejich eliminaci včetně stanovení priorit při jejich realizaci. Bude využito kombinace více testovacích metod, které v maximální míře umožní posoudit úroveň zabezpečení všech komponent testovaného rozsahu informačního systému ze všech dostupných vektorů.

Provedený test bude realizován bez přístupu ke zdrojovým kódům aplikací, se základní sadou oprávnění běžného uživatele.

### 1.3. Způsob připojení

Pro provedení bezpečnostního testu bude použito běžné internetové připojení, které je dostupné uživatelům veřejného internetu v ČR a zahraničí, připojení do LAN bude-li zjištěno během fyzického testu v prostorách MMČB a připojení do wifi sítě/sítí v prostorách MMČB, bude-li získáno v průběhu testu.

### 1.4. Vyloučené kontroly z bezpečnostního testu

Z provedených testů budou vyloučeny veškeré testy, které by mohly mít za následek omezení nebo i jiné poškození dostupnosti služeb testovaných systémů.

### 1.5. Ostatní omezení bezpečnostního testu

Žádná další omezení nejsou stanovena.

## 2. Metodika testu

Kapitola obecně popisuje realizaci jednotlivých fází bezpečnostního testu v režimu „black-box“, což znamená, že provádíme test z prostředí sítě Internet přesně tak, jak by to činili kybernetičtí zločinci, případně s omezeným množstvím informací a bez součinnosti testované organizace. Realistický scénář útoku tak testuje nejen technickou připravenost, ale i lidský faktor v kontextu kybernetické bezpečnosti testované organizace.

### 2.1. Penetrační test

#### 2.1.1. Fáze získávání informací

V této fázi je simulováno chování útočníka a technik v počáteční fázi sběru informací o cíli kybernetického útoku s využitím OSINT (Open source intelligence) a analýza těchto informací, kdy tyto informace slouží k volbě vhodných technik v průběhu fáze enumerace zranitelností

Během fáze získávání informací jsou získány základní informace o testované aplikaci/IS. Fáze získávání informací je složena z několika samostatných částí, mezi které patří sbírání dat, získávání informací apod. K vyhledávaným informacím patří např.

- doménová jména;
- IP adresy;
- informace o ISP;
- vlastníci aplikací, IS a služeb;
- autoři webových aplikací;
- publikované příspěvky zaměstnanců odhalující používané technologie;
- nechtěně publikované informace;
- vazby mezi obchodními partnery apod.

Tato fáze probíhá bez přímého kontaktu s testovanou aplikací nebo IS.

### 2.1.2. Fáze skenování infrastruktury

Fáze skenování představuje neinvazivní způsob zkoumání testované aplikace/IS, která většinou probíhá na síťové a transportní vrstvě. Mezi základní získávané informace patří:

- otevřené, zavřené nebo filtrované síťové porty;
- informace o publikovaných službách;
- identifikace používaných OS;
- základní pravidla chování firewallů, případně ostatních bezpečnostních technologií;
- základní pravidla pro chování síťových technologií pro překlad adres, load balancing, apod.

Na základě informací získaných z této fáze je možné určit další postup provádění bezpečnostních testů, které jsou konzultovány s odpovědným zaměstnancem organizace.

### 2.1.3. Fáze zjišťování stavu systémů a aplikací

Na základě poskytnutých nebo zjištěných informací dochází v této fázi k volbě vhodných technik pro enumeraci známých zranitelností v testovaných technologiích nebo v jejich konfiguracích. Techniky jsou voleny takovým způsobem, aby byl minimalizován negativní dopad na testované technologie.

Tato fáze představuje výzkum identifikovaných zranitelností, slabin nebo nevhodných konfigurací a jejich ověřování na testované aplikaci/IS. K hlavním úkolům této fáze patří:

- určení typů aplikací, IS nebo služeb, které mohou být zranitelné;
- úroveň aplikování opravných balíků;
- seznam možných DoS útoků;
- seznam oblastí, které mohou být zabezpečeny pomocí pravidla Security through obscurity;
- seznam jmenných konvencí na poštovních serverech atd.

Pro získávání vhodných postupů nebo nástrojů na využití těchto zranitelností je možné použít zdroje z Internetu (např. WWW, FTP, IRC služby, Google atd.). Pokud je to nutné nebo vhodné, testeři připravují vlastní postupy a nástroje.

### 2.1.4. Fáze exploitace

Na základě informací a analýzy nalezených zranitelností jsou zvoleny vhodné techniky pro exploitaci nalezených zranitelností v souladu se stanovenými cíli penetračního testu. Může se jednat v závislosti na stanovených cílech a pravidlech penetračního testu pouze o „proof of concept“ pro prokázání nalezených zranitelností a/nebo se může jednat o prvotní fázi průniku s cílem simulovat chování útočníka ve fázi post-exploitace.

Během této fáze jsou využívány dostupné exploity na známé zranitelnosti v technologiích a jejich konfiguracích a v případě potřeby jsou tyto exploity našimi konzultanty modifikovány, aby byla zajištěna jejich funkcionalita v testovaném prostředí. V některých případech je realizován vývoj vlastních exploitů na nalezené zranitelnosti

### 2.1.5. Fáze post-exploitace

Tato fáze slouží po úspěšné exploitaci nalezených zranitelností zejména k simulaci chování útočníka po prvotním průniku do testovaného prostředí s cílem udržení přístupu do prostředí, eskalace privilegií a laterárního pohybu v rámci prostředí a případného získání přístupu mimo IT prostředí.

## 2.2. Test sociálním inženýrstvím

### 2.2.1. Rámování testu

Prioritou před provedením phishingové kampaně je snaha porozumět požadavkům objednatele, a proto provádíme počáteční posouzení a rámování definice a rozsahu phishingové kampaně.

### 2.2.2. Průzkum

Před provedením kampaně se provádí počáteční kybernetický průzkum ve snaze najít informace, které lze využít v přípravné a realizační fázi. Nasbírané informace mohou obsahovat uživatelská jména, e-mailové adresy, aktiva společnosti a další.

### 2.2.3. Verifikace

Jakmile jsou potřebné informace nashromážděny, zahajuje se počáteční analýza organizace, která odhalí informace, jež nám pomohou zajistit vyšší úspěšnost v doručení phishingových útoků.

### 2.2.4. Útok

Jakmile jsou zpracovány všechny vstupy, navrhují se (cílené) phishingové e-maily a provádí se útok zasláním phishingových e-mailů zaměstnancům, které obsahují neškodný simulovaný odkaz/dokument, který má emulovat skutečný malware.

### 2.2.5. Testující strana

Na testující straně budou všechny výsledky prováděné kampaně opatřeny časovým indexem, a uloženy pouze po dobu potřebnou. Po skonční projektu budou data stejně jako veškerá infrastruktura bezpečně odstraněna.

### 2.2.6. Testovaná strana

Testovaná strana není vázána povinností sledovat průběh kampaně. Časovým indexem do standardních Systémových a Aplikačních logů uložené informace však mohou mít po skončení kampaně přidanou hodnotu pro zpětnou analýzu a rekonstrukci událostí.

### 2.2.7. Monitoring průběhu kampaně

V průběhu kampaně bude testující strana sledovat primárně následující parametry kampaně. Naopak testovaná strana díky nim po skončení projektu může provést kontrolu svých systémů a auditních záznamů.

**Povolený odesílatel phishingových e-mailů** je seznam legitimních SMTP serverů, které budou transparentní vůči bezpečnostním ochranám jako jsou e-mailový Anti-Spam nebo Anti-Vir testované strany. Odesílatel phishingové kampaně je následně definován a identifikován:

- IP adresou,
- e-mail adresou,
- názvem hostitele (hostname, FQDN)
- nebo hlavičkou v e-mailu.

**Povolené domény** je seznam „bezpečných“ webových adres, kterým bude prohlížeč nemusí důvěřovat, ale budou testující stranou použity pro ověření odolnosti vybraných zaměstnanců. To znamená:

- prohlížeče/jiné bezpečnostní ochrany mohou varovat před nebezpečnými zdroji (např. Phishing, malware nebo nevyžádaný software),
- prohlížeče/jiné bezpečnostní ochrany mohou varovat před stažením souborů hostovaných v těchto doménách,
    - webové prohlížeče jako je např. Google Chrome ve výchozím nastavení totiž analyzují a odesílají data do společnosti Google, která skrze svoji platformu Google Safe Browsing aktivně varuje před vstupem na takové stránky.

### 2.2.8. Telefonický test

Cílem tohoto testu budou telefonní čísla zaměstnanců získaná ve fázi Průzkumu. Na tato zjištěná telefonní čísla budou směřovány útoky dle různých scénářů, jejichž cílem bude přinutit zaměstnance vyzradit nějakou citlivou informaci (např. svoje přihlašovací jméno a heslo) nebo spustit testovací kód (soubor) simulující malware podobně jako u e-mailového testu.

### 2.2.9. Fyzický test

Na základě informací získaných ve fázi Průzkumu budou učiněny pokusy testerů o neautorizovaný průnik do vnitřních prostor organizace a o připojení testovacích zařízení do datových sítí.

## 2.3. Testovací a hodnotící standardy

Metodiky pro bezpečnostní testování používané konzultanty jsou založeny zejména, nikoliv však výlučně, na následujících metodikách, které se řadí do kategorie “best practice” pro různé typy bezpečnostního testování napříč různými sektory:

- Open Source Security Testing Methodology Manual
- The Open Web Application Security Project
- NIST 800-115
- Common Vulnerability Scoring System
- Center for Internet Security Benchmarks
- Doporučení pro zabezpečení od jednotlivých technologických dodavatelů
- a dalšími.

### 2.3.1. OSSTMM

Dodavatel využívá jako základ pro bezpečnostní testování (tedy včetně penetračních testů) uznávaný mezinárodní standard OSSTMM – Open Source Security Testing Methodology Manual.

Tato metodika byla vytvořena v Institute for Security and Open Methodologies – www.isecom.org a je neustále rozvíjena velkou skupinou profesionálních testerů a specialistů na bezpečnost informačních a komunikačních technologií (ICT).

Metodika OSSTMM pokrývá provádění penetračních testů v jakémkoliv prostředí, kdy tester má stejná práva jako běžný uživatel. Ověřením všech oblastí, které jsou definovány v OSSTMM, je v systému proveden kompletní penetrační test.

OSSTMM nepředepisuje formu ani hloubku prováděných testů. Metodika se soustředí na stanovení základních modelů testování, hlavních oblastí testů a způsobu prezentace zjištěných výsledků.

Metodika vychází OSSTMM a neustále je aktualizována tak, aby odpovídala dnes nejlepším používaným praktikám v oboru bezpečnosti ICT a testování bezpečnosti. Nejvýznamnější zdroje metodiky jsou:

- Normy řady ISO/IEC 27000;
- OWASP (Otevřený standard pro testování webových aplikací – www.owasp.org);
- NIST (National Institute of Standards and Technology – www.nist.gov – pouze dokumenty týkající se testování, nastavování a provozování bezpečnosti ICT).

Metodika OSSTMM definuje doporučený rozsah prováděných testů. Pracovníci dodavatele, kteří se specializují na testování bezpečnosti, neustále rozvíjí, udržují a katalogizují rozsáhlou databázi znalostí a konkrétních postupů. Tyto postupy a znalosti se týkají všech nejpoužívanějších operačních systémů, aplikací, síťových protokolů a obecné teorie ICT.

### 2.3.2. OWASP

Při testování webových aplikací se vychází z metodik, které pochází z projektu OWASP (www.owasp.org – The Open Web Application Security Project). OWASP zahrnuje mnoho různých služeb, např. „OWASP Testing Guide“, „Guide to Building Secure Web Applications and Web Services”, dále OWASP TOP TEN projekt, testovací nástroje, „OWASP Web Application penetration checklist” a mnoho dalších.

Pro testování a prezentaci výsledků bezpečnostních testů webových aplikací je použito metodiky OWASP Testing Guide ve verzi 4.

### 2.3.3. NIST Special Publication 800-115

Jako pomocná metodika pro organizování testování je využíváno doporučení NIST SP 800-115 v některých vybraných částech, konkrétně v:

- posouzení bezpečnosti informací, včetně politik, rolí a odpovědností, využívaných metodik a technik
- identifikaci cílů a jejich analýzu z hlediska potenciálních zranitelností včetně technik vyhledávání v síti a skenování zranitelností

- ověřování existence zranitelných míst
- koordinaci, hodnocení, analýzy a zpracování dat.

### 2.3.4. CVSS

Zjištěné zranitelnosti jsou hodnoceny podle významu. Pro tento účel je využíváno metriky CVSS (Common Vulnerability Scoring System), která je průmyslovým standardem pro ohodnocování závažnosti zranitelností v informačních systémech. Na rozvoj této metriky CVSS dohlíží Forum of Incident Response and Security Teams (FIRST). Aktuální a při hodnocení použitá metodika je ve verzi 3.

Metrika CVSS usnadňuje rozlišení kritických zranitelností od těch méně významných, čehož dosahuje ohodnocováním zranitelných míst na bodové stupnici od 0 do 10, přičemž 0 značí nízký stupeň a 10 naopak vysoký. Hodnocení samotné pak probíhá v několika krocích a je založeno na sérii měření orientovaných na různé skupiny charakteristik té které zranitelnosti.

Zranitelnosti identifikované během skenování zranitelností nebo penetračního testu jsou klasifikovány v souladu s metrikou CVSS BMG (CVSSv3 Base Metric Group - https://www.first.org/cvss/v3-1/). Tato metrika ohodnocení je zvolena s ohledem na její celosvětovou akceptaci v bezpečnostní komunitě a poskytuje vyvážený pohled na celkovou klasifikaci zranitelností.

CVSS BMG zachycuje charakteristiky nalezených zranitelností v osmi základních metrikách, které jsou konstantní v čase a nezávislé na prostředí, kde je aplikace provozována.

Použití metrik CVSS umožňuje sledování trendů vývoje zranitelnost systémů, párování s riziky zjištěnými v rámci analýz rizik a dalšími informaci v rámci systémů pro podporu rozhodování bezpečnostního managementu, jako je spolčeností NGSS provozovaná služba SMC (https://www.ngss.cz/sluzba/14-security-management-center).

## 2.4. Používané nástroje

Všechny používané nástroje splňují několik základních kritérií, které obecně zajišťují vyšší bezpečnost a důvěryhodnost prováděných testů a omezují rizika vznikající při testování produkčních systémů.

Všechny nástroje jsou důkladně testovány na vlastním polygonu s cílem ověřit jejich správné fungování, skutečně vykonávané funkce a možné dopady na testované i okolní části systému.

Všechny klíčové nástroje jsou analyzovány a kompilovány pracovníky dodavatele. Nástroje, u kterého toto není možné, jsou zvýšenou měrou testovány a používají se pouze pro detekční účely, a ne ve fázích vytváření nebo udržování přístupu do testovaného systému.

V případě potřeby použití speciálního kódu na využití existující slabiny (tzv. exploit) jsou vždy preferovány vlastní programy nebo ty, u kterých je možné provést kontrolu zdrojového kódu a otestovat jejich funkčnost na polygonu.

Většina uvedených nástrojů nemá žádný, nebo jen minimální škodlivý dopad na vlastní testované systémy. U nástrojů, kde existuje vyšší riziko, ale kde kvalita a přidaná hodnota nástroje nelze nahradit žádným bezpečnějším způsobem, je toto uvedeno. Použití těchto nástrojů je vždy plánováno na dobu, ve které nejsou produkční systémy příliš využívány.

## 2.5. Opatření pro minimalizaci rizik

Přestože skenování většiny současných technologií na výskyt zranitelností má žádný nebo minimální negativního dopad, nelze u některých technologií negativní dopad zcela vyloučit. Z důvodu minimalizace negativního dopadu volíme zejména tyto postupy:

- Včasné upozorňování na technologie, které mají být předmětem skenování zranitelností a je u nich známé zvýšené riziko negativního dopadu a doporučení alternativního postupu enumerace zranitelností.
- Nastavení automatizovaných nástrojů pro skenování zranitelností takovým způsobem, aby testování minimalizovalo potřebné zdroje na straně testovaných technologií.
- Skenování zranitelností probíhá po dílčích částech.
- V případě, kdy je možné realizovat skenování zranitelností jako white box test, aniž by to negativně ovlivnilo výsledek realizovaného testu, doporučujeme vždy realizaci skenování zranitelností tímto způsobem.

- V případě, kdy je možné realizovat skenování zranitelností v testovacím prostředí, aniž by to negativně ovlivnilo výsledek realizovaného testu, doporučujeme vždy realizaci v testovacím prostředí.
- V případě zjištění, během provádění testů, že testovaná infrastruktura a aplikace byly v minulosti cílem útoku a byly tímto útokem kompromitovány, bude provádění testů přerušeno až do vyřešení vzniklého incidentu. Zástupce společnosti organizace bude o této skutečnosti neprodleně informován.

### 2.6. Závěrečná zpráva

Z bezpečnostního testu bude zpracována závěrečná zpráva v předpokládané následující struktuře (finální struktura může být testerem upravena tak, aby lépe odrážela výsledky testu).

- Manažerské shrnutí zahrnující souhrn zjištění a doporučení k přijetí opatření s indikací prioritizace opatření
- Základní informace o testu včetně časového rámce, cílů, rozsahu, technických údajů, údajů o testovacím týmu, omezeních testu apod.
- Metodika testu popisující fáze testu i použité metriky tak, aby bylo možné test periodicky opakovat, případně ověřit výsledky
- Výsledky penetračního testu se statistickým vyhodnocením a podrobným popisem zjištěných nálezů v testovaném rozsahu systémů, sítí apod.
- Výsledky phishingové kampaně jsou analyzovány a reportovány zpět objednateli v plné míře s identifikací zranitelných míst, náchylnosti zaměstnanců k phishingovým e-mailům a souvisejícími riziky včetně seznamu doporučení.

## 3. Parametry testu

### 3.1. Nastavení prostředí

Externí část testu bude probíhat vzdáleně ze systémů společnosti NGSS prostřednictvím veřejné sítě internet. Test wifi a LAN bude probíhat v prostorách MMČB.

Systémy testera provedou před zahájením testů časovou synchronizaci proti důvěryhodnému časovému zdroji.

Pro zařízení testerů jsou primárně vyhrazeny adresy 85.207.10.109 a 91.245.8.110, případně dle okolností testu i jiné.

### 3.2. Technické parametry a průběh penetračního testu

Technické parametry jsou s ohledem na prostředí stanoveny následovně:

- Maximální počet současně otevřených spojení – 15
- Maximální počet současně testovaných systémů – 1
- Maximální počet současných testů na systém – 3

### 3.3. Sledované hodnoty

#### 3.3.1. Testující strana

Na straně testera budou všechny výsledky prováděných testů opatřeny časovým indexem a uloženy. Sledované výsledky jsou výstupy testovacích nástrojů nmap a nessus. Kompletní záznam síťové komunikace mezi systémem auditora a testovaným systémem bude proveden nástrojem tcpdump a uložen ve standardním formátu pro následné zpracování analytickým nástrojem Ethereal.

Výsledky prováděné kampaně budou opatřeny časovým indexem, a uloženy pouze po dobu potřebnou. Po skončení projektu budou data stejně jako veškerá infrastruktura bezpečně odstraněna.

#### 3.3.2. Testovaná strana

Testovaná strana není vázána povinností sledovat průběh testu. Časovým indexem do standardních Systémových a Aplikačních logů uložené informace však mohou mít po skončení kampaně přidanou hodnotu pro zpětnou analýzu a rekonstrukci událostí.

### 3.3.3. Monitoring průběhu testu

V průběhu testu bude auditor neustále monitorovat dostupnost systému na úrovni ip stacku pomocí icmp dotazů. Vyhodnocována bude kromě existence odpovědí i jejich latence. Současně bude tester provádět dle jeho možností kontroly stavu testovaných aplikací.

Všechny uvedené hodnoty budou v případě zjištěných problémů s odezvou testovaných systémů uvedeny v dokumentu Závěrečná zpráva z testu.

## 3.4. Časový průběh testu

Následující časový harmonogram byl sestaven na základě empirických best-practice metod a dle možností organizace.

Čas T je časem datu účinnosti smlouvy. Termíny předpokládají součinnost klienta se zpřístupněním prostor a poskytnutí ethernet konektivity.

### 3.4.1. Interní test zranitelností

Testování bude zahájeno v do T+14 dní.

Předpokládané ukončení je do T+20 dní.

### 3.4.2. Zpráva z testu

Výsledná souhrnná zpráva z provedených testů bude klientovi předána do T+45 dní.

V případě úspěšného průniku nebo zjištění zásadní bezpečnostní slabiny bude informován odpovědný zástupce testované organizace a bude konzultován další postup testu.

## 3.5. Přístupové údaje

Nebudou poskytnuty.

## 3.6. Komunikační scénář a dohled testovacího prostředí

Test zahájí tester na základě explicitního svolení odpovědné osoby organizace. Toto svolení odpovědná osoba vydává v okamžiku, kdy test prováděný podle této metodiky nemůže negativně ovlivnit fungování organizace

Organizace po celou dobu testu provádí aktivní monitoring systémů a odpovídající části síťové infrastruktury.

V případě události ovlivňujících chod testovaného systému odpovědná osoba neprodleně informuje testera a po vzájemné dohodě v testu pokračují nebo test ukončí.

V případě události ovlivňující vetší množství systémů, produkční systémy nebo významnou část infrastruktury informuje odpovědná osoba testera o této události a zahájí postup podle odpovídajících havarijních plánů. Tester okamžitě testování ukončí.

Po ukončení testování tester informuje odpovědnou osobu o ukončení testu. Odpovědná osoba provede kontrolu systému. V případě technických problémů provede odpovídající havarijní plán nebo plán obnovy.

## 3.7. Riziko infekce škodlivým kódem

Testovací postupy nepředstavují kybernetické riziko (nejsou nositeli škodlivého kódu) a proto není potřeba provádět před spuštěním dodatečná přípravná opatření spojená s ochranou před škodlivým kódem.

## 3.8. Riziko úniku citlivých dat

Práce s daty z průběhu kampaně (uživatelské údaje jako jméno, příjmení, IP adresa, email, pracovní pozice, závěrečná zpráva) bude striktně dodržovat zásady práce s citlivými údaji včetně GDPR regulace. Získané informace z kampaně budou odstraněny již v průběhu testování (např. získaná hesla nebudou ukládána celá, ale pouze částečně pro účel reportu apod.). Výjimky budou definované a uvedené v tomto dokumentu.