Smlouva o dílo

(dále jen „***Smlouva***“)

Číslo smlouvy objednatele: **2024000025**

Číslo smlouvy zhotovitele: **NAB-ROJ-2326868**

Statutární město České Budějovice
se sídlem: nám. Přemysla Otakara II. 1/1, 370 92 České Budějovice
IČO: 00244732
DIČ: CZ00244732
zastoupené: Mgr. Davidem Křížem, vedoucím odboru ICT, na základě plné moci
(dále jen „***Objednatel***“)

-a-

COMGUARD a.s.
se sídlem: Sochorova 3209/38, Žabovřesky, 616 00 Brno
IČO: 04305426
DIČ: CZ29214980
zapsaná v obchodním rejstříku vedeném u Krajského soudu v Brně, oddíl B, vložka 7361
zastoupená Ing. Martinem Votavou, obchodním ředitelem, na základně plné moci

(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. Bezpečnostní audit 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. Testy musí být vedeny z prostředí Internetu mimo síť MMČB, kromě těch částí testování, které vyžadují fyzickou přítomnost testera v prostorách testovaných organizací. 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. Nejzazší datum pro předání Díla je 90 dnů ode dne účinnosti Smlouvy.

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, tj. 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 **180.000,- Kč** (*slovy sto osmdesát 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 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 odst. 12.3, 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 Za porušení povinnosti ochrany informací podle čl. 7 této Smlouvy je Zhotovitel povinen uhradit Objednateli smluvní pokutu ve výši 50 000,- Kč, a to za každý jednotlivý případ porušení této povinnosti. Uplatněním smluvní pokuty není dotčen nárok poškozeného na náhradu škody v plné výši.

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

9.8 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. PROHLÁŠENÍ

11.1. Zhotovitel prohlašuje, že ke dni uzavření Smlouvy jsou informace uvedené v čestném prohlášení (omezující opatření ve vztahu k mezinárodním sankcím), předloženém v jeho nabídce v souladu se zadávací dokumentací veřejné zakázky pravdivé.

11.2. Zhotovitel bez zbytečného odkladu, nejpozději však do 5 pracovních dnů, informuje Objednatele o tom, že se dozvěděl o některé z následujících skutečností:

11.2.1. Zhotovitel nebo jeho poddodavatelé jsou osobami, na které dopadají mezinárodní sankce podle zákona č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů, na základě kterých Objednatel nesmí zadat veřejnou zakázku;

11.2.2. Zhotovitel nebo jeho poddodavatelé jsou osobami, na které dopadají mezinárodní sankce podle zákona č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů, na základě kterých Objednatel nesmí zpřístupnit finanční prostředky za plnění Smlouvy.

11.3. Smluvní strany se dohodly, že v případě porušení povinnosti Zhotovitele dle odst. 11.2.1. nebo 11.2.2. tohoto článku vzniká Objednateli nárok na smluvní pokutu ve výši 100.000 Kč za každý takový případ.

11.4. Objednatel je oprávněn od Smlouvy písemně odstoupit, nastane-li skutečnost předvídaná v odst. 11.2. Smlouvy, o které je Zhotovitel povinen informovat Objednatele.

12. ZÁVĚREČNÁ USTANOVENÍ

12.1. 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.

12.2. 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.

12.3. Smluvní strany berou na vědomí, že za podmínek vyplývajících ze zákona č. 340/2015 Sb., v platném znění, podléhá tato Smlouva uveřejnění v registru smluv, přičemž uveřejnění dle tohoto zákona zajistí Objednatel způsobem, v rozsahu a ve lhůtách z něho vyplývajících. Smluvní strany si ujednávají, že Objednatel je oprávněn bez omezení provést uveřejnění úplného znění této Smlouvy včetně všech příloh v registru smluv i v případě, že povinnost k jejímu uveřejnění ze zákona dle předchozí věty nevyplývá, jakož i uveřejnění na oficiálních webových stránkách města České Budějovice. Smluvní strany berou dále na vědomí, že Objednatel je povinen tuto Smlouvu či skutečnosti z ní vyplývající uveřejnit nebo poskytnout třetím osobám, pokud takový postup vyplývá z příslušných 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.

12.4. Vyhrazená změna závazku:

12.4.1. 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.

12.4.2. 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.

12.5. 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

12.6. 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**
Ing. Martin Votava Digitally signed by Ing. Martin Votava Date: 2024.01.12 15:34:25 +01'00'	Digitálně podepsal Mgr. David Kříž Datum: 2024.01.12 11:08:55 +01'00'
.....	.....
COMGUARD a.s.	**Statutární město České Budějovice**
Ing. Martin Votava	Mgr. David Kříž
Obchodní ředitel	vedoucí odboru ICT

Příloha č.1

Specifikace Díla

PENETRAČNÍ TESTOVÁNÍ IT INFRASTRUKTURY MMČB 2023

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, 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 Internetu mimo síť MMČB.
Předpokládáme, že testy zahrnou následující činnosti:

Identifikace cíle

Sběr z internetu dostupných informací o IT prostředí zadavatele (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 zadavatele

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 zadavatele.

Reakce na testy

Analyzovat případné reakce ochranných nástrojů zadavatele 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 zadavatele

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 nejméně následující kroky:

- provést kontrolu nastavení bezpečné komunikace (např. pomocí https, ssl);
- prověřit bezpečnost kritických datových toků;
- prověřit možnost zneužití aplikací neautorizovaným způsobem, kontrola hodnot při zadání uživatelem;
- provést pokus o získání přihlašovacích údajů registrovaného uživatele;
- prověřit náchylnost na aplikační zranitelnosti definované v rámci projektu OWASP;
- prověřit bezpečnost technologií, na kterých jsou systémy postaveny (operační systémy, webové, aplikační a databázové servery) a bezpečnost jejich integrace do zbývající infrastruktury;
- prověřit možnosti zneužití technologií dostupných v aplikaci útočníkem a otestování hrozby útoku na účty/relace legitimních klientů.
- provést všeobecné posouzení bezpečnostní úrovně;

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 je simulace útoku na přístup do vnitřní sítě organizace prostřednictvím bezdrátového signálu WiFi sítí. Po získání přístupu musí být prověřena kvalita oddělení provozu mezi síťovým segmentem WiFi klientů a zbytkem interní sítě.
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 dodavatele.
Výstupem testu bude přehled a zmapování provozovaných WiFi sítí a seznam bezpečnostních nálezů s následným možným dopadem na vnitřní síť zadavatele.
Součástí testů bude také analýza kvality požadované konfigurace připojení k bezdrátové síti na straně klientských zařízení z pohledu bezpečnosti. K tomuto posouzení poskytne Zadavatel součinnost (vstupní informace).

4. Testy sociálním inženýrstvím

Cílem testu je prověřit úroveň bezpečnostního povědomí zaměstnanců – uživatelů informačního systému zadavatele 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 dodavatel vycházet zejména z údajů dostupných na webových stránkách zadavatele 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 dodavatelem kontrolovaný útok na e-mailové adresy zaměstnanců získané na webových stránkách zadavatele, 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, nebo jej přinutí zadat citlivé údaje o svém účtu nebo o své osobě do odkazované stránky. „Škodlivý“ 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 nebo zadá osobní údaje či jinak citlivé informace.
V rámci testu přepokládáme otestování nejméně 200 náhodně vybraných zaměstnanců úřadu.
Validita zjištěných informací bude následně dle možností ověřována a budou pořizovány důkazy formou screenshotů apod.

4.2. Telefonický test

Cílem tohoto testu budou telefonní čísla zaměstnanců zadavatele získaná na webových stránkách zadavatele 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 50 dodavatelem náhodně zvolených zaměstnanců úřadu.

4.3. Fyzický test

Cílem tohoto testu budou informace o cílových lokalitách zjistitelné na webu zadavatele, 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 zadavatele.
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 společnosti apod. Tyto skutečnosti i průběh testu budou dle možností dokumentovány 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 odboru ICT, který bude v případě odhalení průniku nebo jiné eskalované situace kontaktován a který případně rozkryje prováděný test cílovým zaměstnancům.
Pokud tester nalezne v budovách úřadu veřejně dostupný LAN port, umožňující přístup do vnitřní sítě úřadu, 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 odboru ICT (pouze jemu).

5. Obsah a struktura závěrečné zprávy z testů

Výstupem penetračních testů bude závěrečná zpráva o stavu technické bezpečnosti prověřovaného prostředí a webových 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 hodnotící zpráva s cílem podchytit a stručně a srozumitelně popsat zjištěné výsledky testování a analýz. Cílem manažerského shrnutí je přehledně podat 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 popis postupu provedených testů včetně nástrojů a technik použitých v jednotlivých fázích.
- Detailní popis všech jednotlivých zjištění ze všech fází testů včetně identifikace metody/nástroje, který přispěl k odhalení bezpečnostního problému. Nalezené zranitelnosti budou popsány 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)	Bezpečnostní zjištění zahrnující zejména informace o systémech a sítích publikované bez zřejmého účelu, které 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	Pro zneužití zranitelnosti je potřeba technicky zdatný útočník využívají automatizované či kombinaci automatizovaných a manuálních metod 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, případně aplikaci dostupných bezpečnostních záplat.

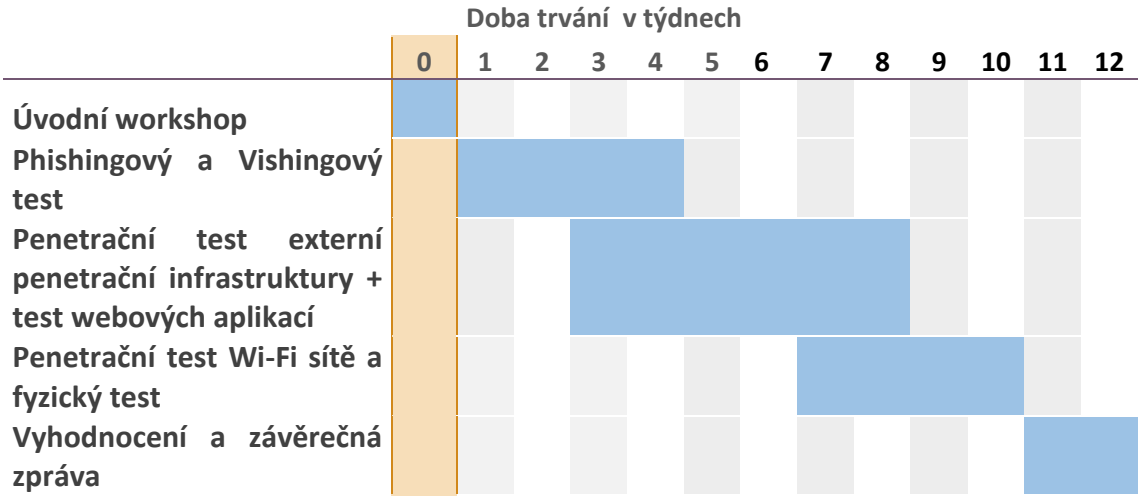
Příloha č. 2

Termíny plnění a harmonogram provedení prací

Harmonogram provedení prací:

Harmonogram zahrnuje provedení všech požadovaných testů (Phishingový, Vishingový, Penetrační test externí IT infrastruktury, penetrační testy webových aplikací, testování Wi-Fi sítě a fyzické bezpečnosti společnosti). Celý harmonogram je rozepsán do několika etap (viz následující diagram). Zahájením projektu se rozumí provedení úvodního workshopu, který bude realizován do 10 pracovních od podepsání smlouvy oběma smluvními stranami. Celý projekt bude realizován během 12 pracovních týdnů od jeho zahájení.

Harmonogram prací:



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: 3/2024

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:
Roman Jiráček, Senior Account & Vendor Manager

za Objednatele:
Mgr. David Kříž, vedoucí OICT

Pro provádění Díla:

za Zhotovitele:
Ondrej Malik, Security Consultant

za Objednatele:
Mgr. David Kříž, vedoucí OICT
Bc. Tomáš Železný, Městská policie České Budějovice

Příloha č. 4

Nabídka Zhotovitele

Příloha č. 4 - Veřejná zakázka č. - VZ1160/2023/008 Penetrační testování IT infrastruktury MMČB 2023

číslo dokumentu	**ROJ-2326868**
datum	15. 12. 2023
zákazník	**Magistrát města České Budějovice**
zpracoval	Roman Jiráček [redacted]

COMGUARD a.s.
Sochorova 38
CZ 616 00 Brno
tel. +420 513 035 400
fax +420 513 035 398
DIČ: CZ04305426
www.comguard.cz

Obsah

PROFIL SPOLEČNOSTI

Společnost COMGUARD a.s působí na trhu jako value added distributor a poskytovatel professional services, který se zabývá kybernetickou bezpečností v České republice a na Slovensku. Díky našemu širokému portfoliu produktů a služeb, jsme Vám schopni poradit nejen v základních oblastech bezpečnosti, jako je ochrana endpointů (antivirová a antimalware řešení), ochrana perimetru, emailové komunikace či mobilních zařízení. Samozřejmostí jsou i oblasti webového provozu či síťové sondy. Zabýváme se také ochranou dat a šifrováním, včetně šifrovaných flash disků a pevných disků či dvoufázovou autentizací. Poskytujeme kompletní ochranu nejen pro malé a střední společnosti, ale i pro nadnárodní společnosti využívající robustní bezpečností nástroje. Pro Vaši infrastrukturu jsme schopni navrhnout a doporučit SIEM řešení, řešení přístupů pro privilegované účty, monitoring nejen administrátorských aktivit, nástroje pro management zranitelností či pro samotné pro odhalení konfiguračních zranitelností.

Certifikace a zkušenosti

Společnost COMGUARD a.s. je držitelem certifikátu managementu informační bezpečnosti **ČSN ISO/IEC 27001:2006** (ISMS) a rovněž je držitelem certifikátu managementu jakosti **ČSN EN ISO 9001:2001** v oboru expertní služby v oblasti informačních technologií, zejména bezpečnosti IT; nákup a prodej hardware, software a komunikační technologie.

K předním výhodám společnosti patří i tým certifikovaných specialistů na technologie v našem produktovém portfoliu. Díky dlouholetým zkušenostem v oblasti kyberbezpečnosti jsou naši experti schopni poskytnout pomoc v jakékoliv oblasti IT bezpečnosti, kterou právě řešíte. Ať už se jedná o návrh nového konceptu bezpečnosti na základě provedeného auditu, profesionální implementace a konfigurace námi distribuovaných produktů, školení či otestování úrovně aktuální bezpečnosti.

Reference

Mezi naše spokojené zákazníky patří společnosti z oblasti telekomunikací, energetiky, zdravotnictví, průmyslu, vzdělávání, bankovního sektoru, výrobních nadnárodních společností i státní správy.

Kompetenční centrum

Kompetenční centrum, které vlastní a provozuje společnost COMGUARD a.s., je zaměřeno na testování, prezentace a návrhy konkrétních řešení v oblasti IT bezpečnosti.

Partneři a koncoví zákazníci z řad podniků a státních institucí mají možnost si otestovat bezpečnostní řešení celosvětově uznávaných výrobců, a to v nasimulovaných reálném provozu. Cílem Kompetenčního centra je informovat zákazníky o nových bezpečnostních

rizicích a dalším vývoji, seznámit je s novými bezpečnostními technologiemi, pomoci jim rychleji na ně reagovat a nastavit jejich řešení i s ohledem na normativní požadavky. Zpětná

vazba od zákazníků a využití jejich zkušeností umožňuje rozvíjet a připravit řešení ušité přímo na míru konkrétním potřebám každého zákazníka.

KVALIFIKAČNÍ PODMÍNKY

Společnost COMGUARD a.s. se sídlem Sochorova 38, Brno 616 00, IČ 04305426 předkládá následující dokumenty ke splnění kvalifikace a požadavků:

Technická kvalifikace

Splnění technické kvalifikace je doloženo následujícím seznamem referencí a projektovým týmem, který se bude na zakázce podílet.

Projektový tým

Jakub Mazal

Ve společnosti COMGUARD působí více než 6 let na pozici Security consultant. Od začátku roku 2016 se specializuje na zabezpečení koncových stanic; ochranu dat; bezpečnost informačních systémů včetně jejich penetračního testování, webového provozu, emailové komunikace, virtualizovaných prostředí. Pravidelně se účastní školení, certifikací a beta testů bezpečnostních produktů.

Mezi jeho referenční projekty lze uvést Nemocnice Jablonec nad Nisou, Hochtief, Česká Zbrojovka, TIPOS SK a mnohé další.

Jan Burian

Ve společnosti COMGUARD působí více než 6 let na pozici Security consultant. Od roku 2015 se specializuje na ochranu webového provozu a emailové komunikace, včetně simulace phishingových útoků. Dále se věnuje komplexní ochraně sítí, bezpečnosti informačních systémů, správa bezpečnostních systémů typu SIEM a podílí se na poskytování služeb v rámci SOC (Security Operation Center). Drží certifikace předních výrobců zmíněných oblastí, pravidelně se účastní školení.

Mezi jeho samostatné referenční projekty, kde lze ve zkratce uvést Energetický průmyslový holding a Generální finanční ředitelství, kde proběhly samostatné kampaně na PhishTest. Mezi další zakázky patří Slovenská akadémia vied, Institut biostatistiky a analýz, Vysoká škola chemicko-technologická a další.

Ondrej Malík

Ve společnosti COMGUARD působí více než 4 roky na pozici Security consultant. Jeho primární specializací je bezpečnost informačních systémů, ochrana dat, penetrační testování systémů a uživatelů, ochrana webů, e-mailové komunikace (včetně simulace phishingových útoků) a celkové IT infrastruktury. Mimo penetrační

testování se zaměřuje na nové technologie zejména deception technology. Drží certifikace předních výrobců zmíněných oblastí, pravidelně se účastní školení.

Mezi jeho referenční projekty patří společnosti ze statního, ale i komerčního sektoru. Ve zkratce lze uvést Dopravní podnik Ostrav, Nemocnice Nové město na Moravě, Subterra. Dále se podílel na projektech pro Energetický průmyslový holding a Generální finanční ředitelství.

POPIS NAVRHOVANÉHO ŘEŠENÍ

Cíle penetračního testování

Cílem penetračního testování je poskytnout společnosti **Magistrát města České Budějovice** (dále jen Zadavatel) ucelený přehled o stavu zabezpečení infrastruktury, resp. její části, která má být testována. Bude prováděno testování externí infrastruktury, webové aplikace, testování Wi-Fi sítě, fyzické bezpečnosti společnosti a sociálního inženýrství – phishing a vishing.
Výstupem z testování bude poukázáno na možnosti zneužití existujících zranitelností, a na možné oblasti vzniku rizik v budoucnosti. Zároveň je cílem penetračního testování i navrhnout jednoznačné kroky k zajištění vyšší úrovně zabezpečení odstraněním existujících problémů, případně návrhy na předejití vzniku podobných problémů.

Etapy penetračního testu

Etapy penetračního testování jsou rozděleny na Stanovení rozsahu, průzkum, řízení a reportování.

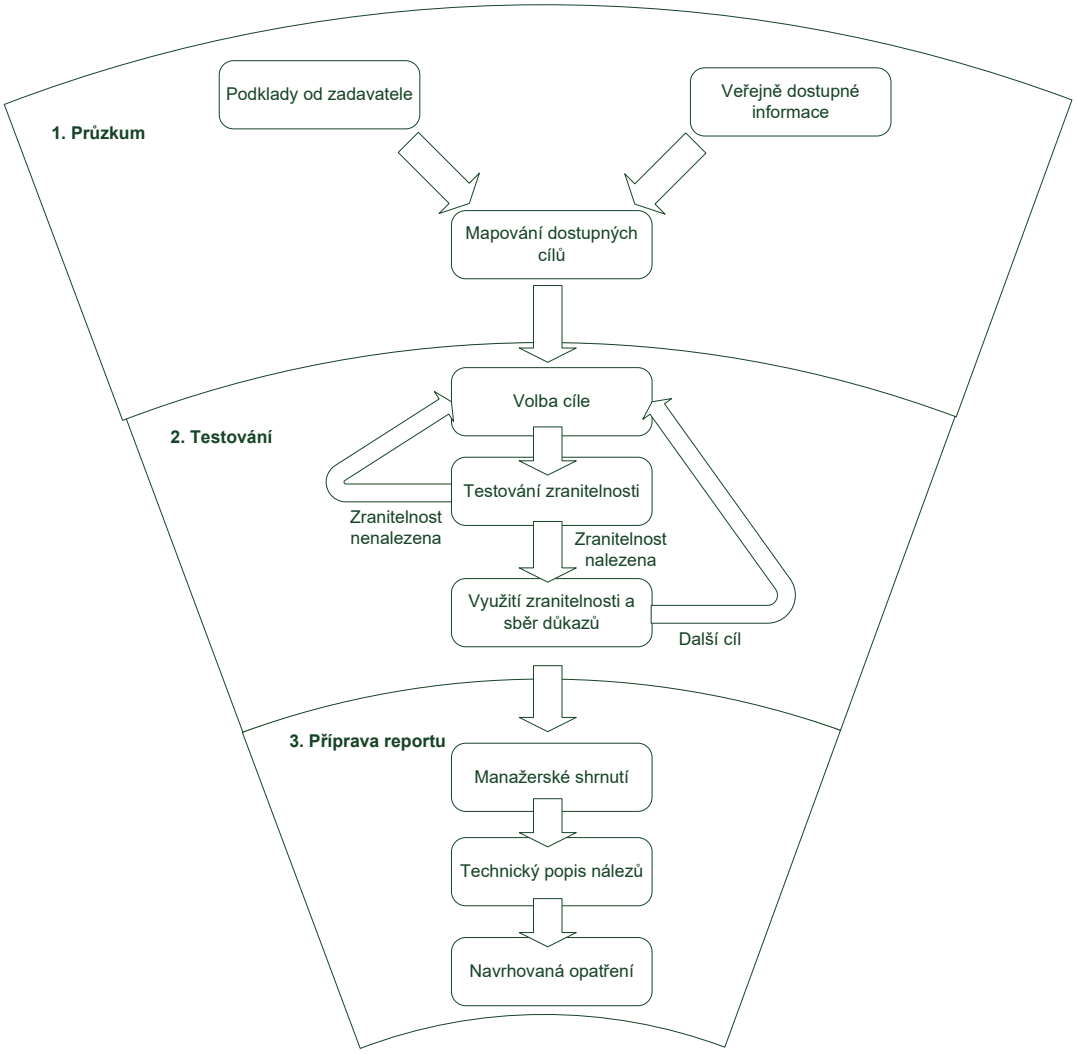
Metodika penetračního testování

Průběh penetračního testování může být proveden dvěma způsoby:

Black-Box Testing – zadavatel poskytne žádné nebo velmi omezené informace a penetrační testování tak simuluje útočníka bez jakékoliv znalosti systému. Výhodou je věrná simulace externího útočníka, nevýhodou potom vyšší pravděpodobnost nenalezení některého z možných cílů.

White-Box Testing – zadavatel poskytne dostatek podkladů, které mohou během testování sloužit jako zdroj informací o cílech testování. Zároveň tyto podklady mohou sloužit k oponentuře použité topologie z bezpečnostního pohledu.

Metodika penetračního testu je zobrazena na následujícím diagramu. Dělí se do tří hlavních fází – průzkum, testování a příprava reportu; jednotlivé fáze jsou rozepsány níže. Předpokládáme testování způsobem „Grey-Box“ Testing, tedy že podkladem bude bližší specifikace síťových rozsahů, informace o topologii a poskytování dalších informací o infrastruktuře.



Obr. č. 1: Etapy penetračního testování

Průzkum – Detailní naplánování bezpečnostního testu

Během této fáze jsou připravovány podklady pro samotné testování a pasivní analýza datových toků v segmentu sítě, kde bude penetrační test probíhat. Budou využity veřejně dostupné informace a další nástroje (manuální nebo semiautomatické) pro získání dodatečných podkladů. Na základě získaných informací jsou zmapovány cíle pro následnou fázi testování.

Použité nástroje a postupy

Použité nástroje jsou vybírány tak, aby byly maximálně efektivní pro jednotlivé fáze penetračního testu. Jsou kombinovány **komerční** i **open-source** nástroje tak, aby prováděné testy vedly k odhalení problémů, ale zároveň je kladen důraz na rychlost provádění testů a tím i celkové snížení nákladů. Testy probíhají v souladu s Open Source Security Testing Methodology Manual.

Životní cyklus projektu – nástroj pro udržování informací a dokumentaci během životního cyklu celého penetračního testu. Bez kvalitní správy nalezených cílů, zranitelností a provedených testů dochází během penetračního testu často zbytečně k opakujícím se úkonům a zároveň bývají opomenuty některé cíle nebo podstatné testy.

Mapování cílů – sada nástrojů pro skenování portů, služeb a aplikací. **Testování zranitelností** – zranitelnosti jsou vyhledávány více možnými způsoby, od plně automatických nástrojů (výhodou je otestování širokého spektra vstupů za velmi krátký čas) po manuální útoky (převážně na konkrétní aplikace), kdy jsou veškerá odesílaná data ručně modifikována, aby byla odhalena nebo potvrzena konkrétní zranitelnost s maximální přesností.

Řízení (koordinace) a provedení vlastního testování

Během testování jsou postupně vybírány cíle, které penetrační tester podrobuje zkoumání za pomoci různých nástrojů (automatických, semiautomatických a manuálních). Pokud je nalezeno chování, které by mohlo ukazovat na přítomnost zranitelnosti, je následně provedena série testů, která má za úkol ověřit možnost jejího zneužití. Při ověřování zranitelností je kladen velký důraz na to, aby nebyla ohrožena stabilita služby nebo integrita a důvěrnost dat (např. pokud je objevena zranitelnost, která umožňuje útočníkovi získat uživatelské jméno a heslo, bude toto demonstrováno pouze na uživatelském jméně a heslo nebude zahrnuto v žádném z výstupů testování).
Během testování může dojít k objevení dodatečných cílů, které nebyly zmapovány během průzkumné fáze. Takové cíle jsou do testování dodatečně zahrnuty. Po vyčerpání a zdokumentování všech cílů je testování ukončeno a výstupem jsou podklady pro tvorbu reportu.

Reportování výsledků v dohodnutém tvaru a harmonogramu

Report penetračního testu obsahuje zpravidla tři typy informací:

- **Manažerské shrnutí** – podává základní přehled o průběhu testu, vyhodnocení úrovně zabezpečení testovaného objektu a obecná doporučení pro zvýšení úrovně zabezpečení. Přehledně mapuje nejrizikovější oblasti.
- **Technický popis nálezů** – detailní popis zranitelností a potenciálně nebezpečných konfigurací kategorizovaný podle nebezpečnosti, které byly během testu identifikovány. Součástí popisu je informace o tom, kde se zranitelnost vyskytuje, jak ji zneužít a co může útočník zneužitím zranitelnosti získat.
- **Navrhovaná opatření** – opatření se týkají vždy konkrétního nálezu, v reportu jsou navrženy konkrétní série kroků pro odstranění dané zranitelnosti, případně snížení pravděpodobnosti jejího zneužití (např. nutná verze softwaru nebo softwarového modulu).

Závěrná zpráva bude obsahovat:

- Průběh testu
- Použité techniky a nástroje
- Objevené slabiny a zranitelnosti
- Kompromitované účty

- Doporučení k nápravě
- Manažerské shrnutí

Veškeré reporty budou vytvářeny na základě cílů a priorit zadavatele.

Součinnost zadavatele

V závislosti na zvolené metodě (Black/Grey/White-Box Testing) poskytne zadavatel údaje o objektech testování v dohodnutém rozsahu.

Dále zadavatel poskytne **Autorizační dokument**, který bude deklarovat požadavek na provedení penetračního testu a zároveň bude obsahovat seznam omezení a podmínek, za kterých je možné penetrační test provádět. Penetrační testování nebude před oboustranným odsouhlasením autorizačního dokumentu zahájeno.

Součástí autorizačního dokumentu budou aspoň následující informace:

- **jaké objekty a aplikace jsou cílem testování (seznam IP adres, portů, atd.),**
- že testování bude vedeno jen pomocí neintrusivních testů (neměly by způsobit nedostupnost služby),
- v jakých časech smí být testování prováděno,
- součinnost, např. správce technologického centra (fyzické umístění sond a penetračních nástrojů v datových centrech), apod.

Dalšími požadavky na součinnost jsou:

- Součinnost správce technologického centra (fyzické umístění sond a penetračních nástrojů v datových centrech).
- Součinnost správce infrastruktury (fyzické připojení sond a penetračních nástrojů do sítí, kde budou penetrační testy prováděny, IP adresy pro sondy a penetrační nástroje, topologie, aplikační prostředí, zřízení vzdáleného přístupu na sondy a penetrační nástroje).
- Součinnost bezpečnostního manažera (konzultace nad stávajícím zabezpečením infrastruktury, v rámci Black/Grey/White-Box Testingu.
- Součinnost na úrovní poskytnutí seznamu emailových adres, konzultaci ohledně grafické podoby phishingové kampaně a zařazení domény, ze které budeme odesílat phighingovou kampaň, na white-list emailové ochrany společnosti (cílem je testovat uživatele nikoliv emailové zabezpečení).
- Součinnost na úrovni poskytnutí základních informací o zaměstnancích, na které bude cílen vishingový test, tzn. jméno, telefonní číslo, značka NTB/PC a výjimku na úrovni anti-malware ochrany (cílem je testovat uživatele a nikoliv bezpečnostní prvky PC/NTB).

ROZSAH PENETRAČNÍCH TESTŮ DLE POŽADAVKŮ ZADAVATELE

Součástí naší nabídkové ceny (viz níže) jsou penetrační testy v rozsahu požadovaném zadavatelem, tedy externí penetrační test infrastruktury, WiFi sítě, fyzický test, webové aplikace, phishing a vishing.

Způsob provádění testů:

Prováděný penetrační test klade důraz na automatizaci testování. Manuálně jsou ověřovány pouze velmi významné nálezy, aby se u nich zamezilo riziku falešné detekce. Většina testování je prováděna kombinací různých automatických a semiautomatických nástrojů.

Externí penetrační test

Postup při provádění Externího penetračního testu

Průzkum

- Pasivní analýza datových toků v segmentu sítě, do níž bude útočník připojen
- Identifikace systémů a služeb, které jsou z daného síťového segmentu dostupné
- Pokus o identifikaci jejich operačního systému a verzí služeb

Testování

- Na základě informací o cílech útoků z fáze rekognoskace realizování testování jejich zabezpečení pomocí:
    - automatizovaných nástrojů
    - manuálních postupů cílených na potenciální zranitelnosti identifikované v předešlé fázi, a na zranitelnosti, které automatizované nástroje nejsou schopny odhalit

Dokumentace

- Výsledky testů jsou zaznamenány do standardizovaných šablon pro jednotlivé identifikované a testované systémy
- Součástí dokumentační fáze je vytvoření sumarizace zajištění pro vedení organizace
- Vytvoření detailní technické zprávy s popisem hlavních zranitelností spolu s odhadem úsilí na jejich odstranění
- Závěrečná zpráva bude vytvořena v českém jazyce
  Penetrační test webové aplikace

Cílem penetračního testu webové aplikace a souvisejících služeb je nestandardními akcemi uživatele demonstrovat zranitelnosti, kterými je možno realizovat průnik do interní infrastruktury zadavatele nebo získat citlivá data či upozornit na chyby v aplikační logice testované aplikace. Test je prováděn zpravidla v režimu black-box, tj. pouze se znalostí webové adresy aplikace. Realizovány jsou jednak automatizované testy zranitelností, tak i manuální testy dle interních postupů s využitím specializovaných nástrojů.
V rámci testu jsou realizovány následující činnosti:

- Kontrola nastavení bezpečné komunikace (např. pomocí https, ssl).
- Náchylnost k DoS/DDoS útokům.
- Chyby aplikační logiky (výpočty, náhodné chyby, ztráta dat).
- Možnost zneužití aplikace neautorizovaným způsobem – chyby v autentizaci, XSS, SQL Injection.
- Zneužití komponent se známými zranitelnostmi.
- Získaní citlivých informací z testované aplikace.
- Pokus o získání přihlašovacích údajů registrovaného uživatele.
- Testy podpůrné infrastruktury webové aplikace (např. API, backend systémy a databáze) a jejich bezpečná integrace v rámci testované aplikace.
- Návrh nápravných opatření a závěrečná zpráva.

Testovány budou aplikace www.c-budejovice.cz, www.inbudejovice.cz, mpolicie.c-budejovice.cz.

Metodika a standardy

V závislosti na typ prováděného testu vycházíme z následujících standardů:

- OWASP – The Open Web Application Security Project
- OSSTMM – The Open Source Security Testing Methodology Manual
- PTES – Penetration Testing Execution Standard

V doporučeních přihlížíme ke stanoviskům institutu NIST – National Institute of Standards and Technology a asociace ISACA – Information Systems Audit and Control Association.

Používané nástroje

Nástroje jsou vybírány na základě struktury sítě a použitých technologiích. Z komerčních nástrojů bývá využíván: Burp Suite Professional, Rapid7 Insight AppSec. Z open source nástrojů bývá využíván například: metasploit, sqlmap, Nmap, OpenVAS, tcpdump, WireShark, Hydra, aircrack-ng, evilginx a další nástroje Kali Linux. Pro některé úzce specializované testy využíváme také interně vyvíjené nástroje.

Postup testování

Samotné testování se skládá z 6 etap, přičemž některé z nich mohou být v závislosti na režimu testování suplovány klientem. Doporučenou 7. etapou pak může být Re Test sloužící k ověření přijatých opatření.

1.) Sběr informací

V první fázi je pozornost zaměřena na získávání informací, podle kterých budou v následujících fázích definovány testovací scénáře proveditelné u zadavatele. Pozornost je zaměřena primárně na hardwarová a softwarová aktiva, případně také na lidské zdroje, které by mohly být během testu využity k úspěšnému narušení bezpečnosti. Tato fáze zahrnuje především aktivní skenování sítě, serverů a dalších aktivních prvků a detekci používaných služeb.

2.) Hodnocení aktiv a identifikace cílů

Druhá fáze je zaměřena na ohodnocení aktiv dle typu OS/firmware, citlivosti uložených dat, otevřených portů a podobně. Kritickým aktivům je přiřazena nejvyšší priorita pro testování. Z takto ohodnocených aktiv jsou identifikované potenciální cíle a scénáře pro penetrační testy.

3.) Identifikace zranitelností

Proces identifikace zranitelností spočívá v objevování slabých míst v aktivech – konkrétních systémech, které mohu být využity pro narušení bezpečnosti zadavatele (např. ve formě průniku, nedostupnosti služeb, neoprávněnému zpřístupnění – pozměnění dat). Způsob identifikace zranitelností je závislý na použitých technologiích a zjištěných informacích. V této fázi jsou typicky používány automatizované nástroje pro nalezení známých zranitelností. Speciální pozornost je pak věnována nesprávné konfiguraci např. nezabezpečenému přenosu citlivých informací či použití slabých šifrovacích a autentizačních schémat.

4.) Verifikace zranitelností a pokus o narušení bezpečnosti

Pokus o narušení bezpečnosti představuje snahu o využití nalezených zranitelností pro neautorizovaný přístup, eskalaci uživatelských privilegií, nedostupnost služby a další nepřátelské akce vůči systémům zadavatele. Při průniku se postupuje s nejvyšší obezřetností, aby nedošlo k poškození anebo znehodnocení testovaných služeb. Cílem všech uskutečněných testů je ověření nalezených zranitelností spolu s individuálními chybami nenalezenými pomocí automatizovaných nástrojů.

5.) Identifikace dopadů po zneužití zranitelnosti

Po úspěšném narušení bezpečnosti je potřebné přezkoumat dostupná data, oprávnění a možnosti dalšího zneužití potenciálním útočníkem. Na konci této fáze dochází k odstranění všech testovacích účtů pořízených pro potřeby testování a také škodlivého, případně nestandardního zdrojového kódu, zaslaného na testované služby.

6.) Tvorba závěrečné zprávy

Závěrečná zpráva včetně manažerského shrnutí obsahuje detailní popis testování, sumarizaci nalezených zranitelností a bezpečnostních mezer, ohodnocení jejich závažnosti, dopadů a rizik. Definuje doporučení k eliminaci zranitelností a minimalizaci rizik.

Závěrečná zpráva

Závěrečná zpráva je výstupem každého našeho penetračního testu. Přináší strategické informace a přehled o slabých místech využitelných k průniku do testovaných systémů. Definuje stupeň jejich závažnosti a navrhuje nápravná opatření k jejich eliminaci.

Nalezené bezpečnostní nedostatky a zranitelnosti jsou klasifikovány pomocí pětibodové stupnice, která zachycuje úroveň rizika (informativní / nízká / střední / vysoká / kritická) dle metodiky CVSS. V případě zjištění kritické nebo vysoké zranitelnosti v průběhu penetračního testování jsou tato zjištění sdělována odpovědným osobám zadavatele bezodkladně.

Postup provedení testu Wi-Fi sítě:

- Simulace útoku na přístup do vnitřní sítě organizace prostřednictvím bezdrátového signálu Wi-Fi sítí.
- Pokus o zjištění dostupných služeb z Wi-Fi sítí apod.
- V případě otevřených Wi-Fi sítí (veřejné, nebo se známým heslem) bude otestována izolace těchto sítí od interních systémů. Cílem je zjistit, zdali útočník nemůže přes otevřené sítě poškodit interní síť zadavatele, nebo poškodit jeho reputaci.
- Přehled a zmapování provozovaných Wi-Fi sítí a seznam bezpečnostních nálezů s následným možným dopadem na vnitřní síť.

Fyzický test

Cílem tohoto testu bude získat informace o cílových lokalitách, kdy bude Poskytovatel čerpat informace veřejně dostupné (web Zadavatele a jinde na internetu) anebo je získá při fyzické obhlídce daných lokalit.

Etický hacker bude vystupovat v roli technické podpory některého z výrobců, které využívá Zadavatel v rámci své IT infrastruktury.
Realizace fyzického testování:

- pokus o fyzický průnik vnitřních prostor lokalit zadavatele
- Získat přístup k prostředkům informačního systému, přístup k citlivým informacím Zadavatele
- Z testování bude vypracován popis samotného průniku, spolu s důkazným materiálem. Pokud to bude situace umožnovat, budou z průběhu vyhotoveny audio-vizuální výstupy (fotky, nahrávky, videa)
  Testy sociálním inženýrstvím – phishingové kampaně

Pro prostředí zákazníka bude provedena phishingová kampaň, která bude odpovídat prostředí zákazníka a bude tak co nejpodobnější interní komunikaci, kterou uživatelů používají při běžné praxi. Phishingová kampaň bude rozeslána prostřednictvím e-mailu.

Obsah služby - PhishTest

Nabízená služba obsahuje:

- Přípravu a provedení **phishingových kampaní**:
  - Příprava kampaní bude probíhat v koordinaci s určeným zástupcem zákazníka;
  - Jednotlivé kampaně se budou od sebe lišit a upravovat dle cílové skupiny uživatelů např.:
    - podvržený email pro běžné služby typu Office365, dropbox,... (obsahující link);
    - email specifický přímo pro skupinu uživatel a geolokaci;
    - vytvoření přílohy nesoucí malware.
- Sběr dat v průběhu kampaně
  - Jednotlivá kampaň probíhá přibližně 1 až 2 týdny (v závislosti na počtu testovaných uživatelů)
  - Testující e-maily jsou dle domluvy buď rozeslány současně, či v předem domluveném časovém rozmezí

- **Vyhodnocení těchto** kampaní vč. manažerského reportu obsahující:
  - Vyhodnocení sběru dat na proprietární platformě Dodavatele;
  - **Detailní statistiky** (např.: počet odeslaných emailů, počet otevřených emailů, počet prokliků na podvržený link, počet získaných přihlašovacích údajů od adresáta)
  - Určení rizikových uživatelů.

Příprava a vyhodnocování kampaní

Ve spolupráci se zákazníkem bude připravena individuální phishingová kampaň, která bude co nejvěrněji odpovídat prostředí a zvyklostem uživatelů (stylu interní komunikace). Phishingová kampaň bude rozeslána prostřednictvím emailu.

Zákazník si může zvolit:

- **Požadovaný scénář** (např. aktualizace credentials pro přístup k internímu systému aj.);

- **Formu distribuce** – odkaz (nejčastější) či zaslání dokumentu;

Phishingové testy lze upravit dle přání zákazníka a jeho aktuálních potřeb. Dále uvádíme základní varianty, které jsou využívány nejčastěji.

Možné základní varianty phishingových kampaní:

A) Standardní Phishingová kampaň

- Vytvoření **phishingového emailu** na běžné služby jako office365, drobbox,... **(nesoucí link)**
- Vytvoření podvržené stránky (z předpřipravených šablon)
- Rozesílka na vybrané uživatele
- Sběr dat
- Závěrečná zpráva

B) Phishingová kampaň - customizovaná

- Vytvoření custome **phishingového emailu** dle požadavků a prostředí zákazníka **(nesoucí link)**
- Vytvoření podvržené stránky (customizované – odpovídající běžnému prostředí zákazníka)
- Rozesílka na vybrané uživatele
- Sběr dat
- Závěrečná zpráva

C) Phishing kampaň s "malware" přílohou

- Vytvoření kampaně dle dohody se zákazníkem
- Vytvoření **přílohy nesoucí malware**
- Rozesílka na vybrané uživatele
- Sběr dat
- Závěrečná zpráva

Sběr dat pro vyhodnocení kampaně:

V rámci phishingové kampaně za účelem jejího vyhodnocení jsou sbírána data následovně:

- Defaultně jsou zaznamenávána jenom **uživatelská jména**.
- Pouze s předchozím souhlasem zákazníka, lze sbírat i hesla
  - např. pro kontrolu, že opravdu došlo k použití validních údajů
- Podvržený malwarový soubor neobsahuje žádný malware rizikový pro infrastrukturu.
  - Využívá pouze principu např. povolení stažení maker v podvodném souboru.
- V případě potřeby lze sepsat NDA.

Vyhodnocení a závěrečný report:

Po proběhnutí individuální phishingovou kampaně následuje vyhodnocení celé kampaně s přehledným grafickým zobrazením statistik. Ukázka statistik je spolu s ukázkami podvržených e-mailů zobrazena v kapitole ***Chyba! Nenalezen zdroj odkazů.***.

V rámci kampaně jsou zjišťovány informace, týkající se uživatelů, vůči kterým byla kampaň spuštěna:

1. **Zda byl e-mail zobrazen** – tato informace byla zjišťována pomocí obrázku vložených v e-mailu, které byly načítány z externích zdrojů. Informace mohla být zjištěna pouze v případě, že bylo zobrazení obrázků uživatelem povoleno,
2. **Zda uživatel otevřel odkaz zaslaný v e-mailu** – tato informace byla zjišťována pomocí unikátního odkazu v každém e-mailu,

3. **Zda uživatel vyplnil přihlašovací údaje do falešné kopie přihlašovací stránky** – tyto údaje lze dohledat a zkontrolovat, zda jsou přihlašovací údaje funkční

V případě zájmu ze strany zákazníka a po jeho odsouhlasení, lze výstupem předat report se jmenným uvedením rizikových uživatelů.

Doporučené varianty PhishTest pro Vaši instituci:

Phishingová kampaň - customizovaná

- Vytvoření custome **phishingového emailu** dle požadavků a prostředí zákazníka **(nesoucí link)**
- Vytvoření podvržené stránky (customizované – odpovídající běžnému prostředí zákazníka)
- Rozesílka na vybrané uživatele
- Sběr dat
- Závěrečná zpráva

Phishing kampaň s "malware" přílohou

- Vytvoření kampaně dle dohody se zákazníkem
- Vytvoření **přílohy nesoucí malware**
- Rozesílka na vybrané uživatele
- Sběr dat
- Závěrečná zpráva
  Testy sociálním inženýrstvím – vishing

Pro účely testů bude využita infrastruktura dodavatele a ověřené volně dostupné nástroje nebo vlastními silami vyvinuté programy. Infrastruktura zákazníka **nebude** ohrožena reálným malwarem.

Jako důkazy provedených útoků budou pořízeny screenshoty, uložena hesla a předány odcizené soubory. Tato data budou po ukončení testů a předání dokumentace odstraněna a nezůstanou ve vlastnictví dodavatele.

Pro celý rozsah testů bude vzájemně odsouhlasen autorizační dokument, který bude popisovat možnosti dodavatele při testování.

Pro efektivitu testování navrhujeme otestovat 15 zaměstnanců MMČB, jelikož v případě, že bychom testovali cca 50 uživatelů, tak si tito uživatelé mohou s větší pravděpodobností předat informaci o probíhajícím vishingovém testu, čímž by celé testování mohlo být ohroženo. S našim předešlých projektů víme, že vzorek 15 uživatelů je dostačující pro naplnění cílů – ověření odolnosti uživatelů vůči útokům typu vishing

Získání užitečných dat z veřejně dostupných zdrojů

- Cílem je mapování struktury organizace, vytipování cílů a zjištění dostatku informací k vytvoření jejich profilu potřebnému k dalším útokům
  - Domény, přístupové portály, login stránky, dodavatelé, interní procesy
  - Sociální sítě (Facebook, Linkedin, Twitter)
  - Google
- Na základě dohledaných informací zjistíme maximum informací o provozované infrastruktuře (OS serverů, provozované služby, bezpečnostní software), topologii sítí zákazníka (pomocí OSS nástrojů, z hlaviček mailové komunikace atd.). Následně zjistíme strukturu společnosti a užitečné kontakty (vedení společnosti, IT administrátoři, účetní oddělení, helpdesk apod.) pro další útoky využívající metody sociálního inženýrství

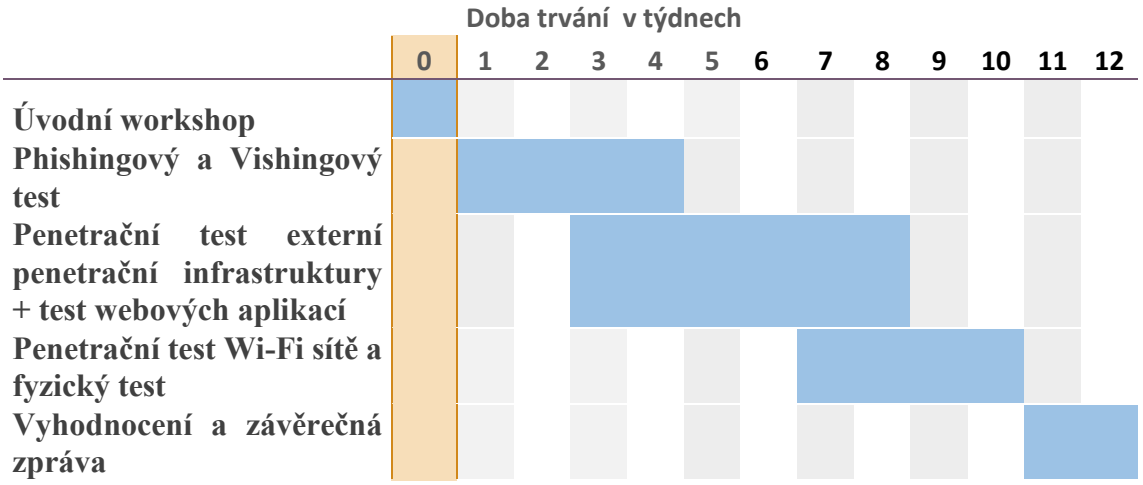
Provedení Vishingových testů

- Z veřejně dostupných informací bude testovaným osobám proveden telefonický hovor za účel získání informací. Využity budou různé scénáře v rámci kterých je cílem získat citlivé informace, od interních hesel k wi-fi sítě až po sofistikovanější informace.
- **Scénář:**
    - Etický hacker zavolá vybranému uživateli a představí se jako technik od výrobce počítače. Útočník si ověří několik osobních informací pro zvýšení důvěry (firma, ve které uživatel pracuje, značka notebooku).
    - Následně ho informuje o tom, že zachytil možný únik informací z jeho zařízení anebo jiný problém a na vyřešení tohoto problému bude nutné stáhnout diagnostický nástroj. Uživatel bude navigovaný na phishingovou doménu , která bude připomínat support daného výrobce notebooku, např. diagnostika-dell.cz- z Této domény bude stažený .exe soubor. Po spuštění se uživateli ukáže výpis opravy, např.:
        - Analyzing 10%
        - Analyzing 20% apod.
        - Fixing problems 10% apod.
    - Tento program spustí reverzní shell na adresu dodavatele. Útok bude úspěšný, pokud se podaří navázat shell session na zařízení daného zaměstnance. Jako důkaz bude v předem určené složce vytvořený soubor poh.txt (proof.of-hack).

HARMONOGRAM PRACÍ A ČASOVÁ NÁROČNOST

Harmonogram zahrnuje provedení všech požadovaných testů (Phishingový, Vishingový, Penetrační test externí IT infrastruktury, penetrační testy webových aplikací, testování Wi-Fi sítě a fyzické bezpečnosti společnosti). Celý harmonogram je rozepsán do několika etap (viz následující diagram). Zahájením projektu se rozumí provedení úvodního workshopu, který bude realizován do 10 pracovních od podepsání smlouvy oběma smluvními stranami. Celý projekt bude realizován během 12 pracovních týdnů od jeho zahájení.

Harmonogram prací:



Pro dodržení harmonogramu je potřeba poskytnout požadovanou součinnost ze strany Zadavatele. Pokud dojde k vícepracím z důvodu nepřesného zadání, nebo špatné organizaci, či neposkytnutí součinnosti ze strany Zadavatele, bude projekt úměrně tomu opožděn. Posloupnost jednotlivých etap projektu, a jejich překryv je možné přizpůsobit dle vzájemné domluvy zadavatele a zhotovitele.

Časová náročnost celého projektu:

Popis prací	On – site MD	Off – site MD
Phishingový test		4
Vishingový test		3
Externí test IT infrastruktury + test webových aplikací		6
Test Wi-Fi sítě + fyzický test	2	1
Obsah a struktura závěrečné zprávy z testů		2
Celková náročnost v MD	**2**	**16**

CENOVÁ NABÍDKA

Cenová nabídka za projekt obsahuje všechny náklady spojené s provedením projektu.

Celková cena v Kč bez DPH	**180 000,-**
DPH 21% v Kč	37 800,-
Celková cena v Kč s DPH	**217 800,-**

ZÁVĚR

Vážíme si skutečnosti, že jsme mohli pro Vaši společnost připravit nabídku a věříme, že naše nabídka splňuje všechny Vaše požadavky.
V případě nejasností či případných dalších požadavků nás prosím neváhejte kontaktovat.
Těšíme se na další spolupráci s Vámi!

Roman Jiráček
Senior Account & Vendor Manager

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel: +420 513 035 400 www.comguard.cz
přímý tel: [redacted] [redacted] [redacted]