SMLOUVA O DÍLO

Název: Dopravní podnik města Ústí nad Labem a.s.
IČO: 250 13 891
Sídlo: Revoluční 26, 401 11 Ústí nad Labem
Zastoupený: Ing. Libor Turek, Ph.D., výkonný ředitel společnosti

(dále jen jako „**Objednatel**“ na straně jedné)

a

Název: AUTOCONT a.s.
IČO: 04308697
Sídlo: Hornopolní 3322/34, 702 00 Ostrava
Zastoupený: Ing. Zdeněk Chobot, Ředitel regionálního centra, na základě plné moci, jejíž ověřená kopie je přílohou č. 2 této smlouvy

(dále jen jako „**Zhotovitel**“ na straně druhé)

uzavírají níže uvedeného dne, měsíce a roku podle § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, tuto

smlouvu o dílo (dále jen „**Smlouva**“)

I.
Předmět Smlouvy

Zhotovitel se touto smlouvou zavazuje provést na svůj náklad a nebezpečí pro objednatele za podmínek níže uvedených dílo: **Penetrační test webového portálu dle nabídky a rozsahu v příloze č. 1** (dále jen „Dílo“) a objednatel se zavazuje Dílo převzít a zaplatit za něj Zhotoviteli cenu, která je sjednána v čl. II této Smlouvy.

II.
Cena Díla

Cena Díla je stanovena dohodou smluvních stran podle zákona č. 526/1990 Sb. o cenách, ve znění pozdějších předpisů a činí 280 000 Kč bez DPH. Cena Díla bude navýšena o DPH podle platných právních předpisů v době uskutečnění zdanitelného plnění.
Cena Díla se skládá z těchto samostatných částí:

Penetrační testy webového eshopu EOS, včetně 1 retestu	107 000 Kč bez DPH
Penetrační testy mobilní aplikace EOS, včetně 1 retestu	121 000 Kč bez DPH
Penetrační testy zabezpečení komunikačního kanálu	52 000 Kč bez DPH

III.
Platební podmínky

Zhotovitel je oprávněn vystavit fakturu po předání a převzetí samostatných částí Díla bez vad a nedodělků. Faktura musí být vystavena nejpozději do 10 dnů po skončení po předání a převzetí samostatných částí Díla bez vad a nedodělků. Smluvní strany se dohodly na bezhotovostním placení z účtu Objednatele na účet Zhotovitele. Platba se uskuteční v korunách českých na základě faktury - daňového dokladu, se splatností 30 dnů od doručení faktury Objednateli. Daňový doklad

musí obsahovat veškeré náležitosti v souladu se zákonem č. 235/2004 Sb. ve znění pozdějších předpisů.

V případě, že faktura vystavená Zhotovitelem nebude obsahovat náležitosti dle této Smlouvy, je Objednatel oprávněn fakturu vrátit Zhotoviteli, přičemž po doručení opravené faktury začne znovu od počátku běžet lhůta její splatnosti.

Povinnost Objednatele zaplatit je splněna dnem odepsání příslušné finanční částky z účtu Objednatele.

IV.
Termín zhotovení díla

Smluvní strany se dohodly, že Dílo bude Zhotovitelem provedeno v těchto termínech:

Penetrační testy webového eshopu EOS, včetně 1 retestu	Nejpozději do 30 dnů od účinnosti smlouvy
Penetrační testy mobilní aplikace , včetně 1 retestu	Nejpozději do 60 dnů od účinnosti smlouvy
Penetrační testy zabezpečení komunikačního kanálu	Nejpozději do 30 dnů od účinnosti smlouvy

Objednatel předal Zhotoviteli při podpisu této smlouvy následující věci a jiné podklady určené k provedení díla:

- přístupy do infrastruktury nutné pro provedení testu
- informaci o časech, kdy je možné testovat
- kontakt na technický support objednatele pro řešení případných problémů vzniklých během testování

Převzetí výše uvedených věcí a podkladů Zhotovitel tímto Objednateli potvrzuje.

IV.
Předání a převzetí Díla

K předání a převzetí samostatných částí Díla dojde do dvou dnů od jejich zhotovení, nejpozději však budou samostatné části Díla zhotoveny i předány v termínu uvedeným v čl. IV této smlouvy.

O předání a převzetí samostatných částí Díla bude Smluvními stranami vyhotoven písemný předávací protokol.

V.
Odpovědnost za vady

Zhotovitel se zavazuje předat Dílo bez vad a nedodělků.

Smluvní strany se dále dohodly, že budou-li v době předání na Díle zjevné vady či nedodělky, k předání a převzetí Díla dojde až po jejich odstranění. O této skutečnosti bude Smluvními stranami sepsán záznam. Náklady na odstranění vad nese Zhotovitel.

Výše uvedeným ujednáním není dotčena odpovědnost Zhotovitele za vady Díla, které jsou při předání a převzetí Díla skryté a projeví se později. Tyto skryté vady Díla je Objednatel oprávněn vytknout Zhotoviteli a uplatnit u něj nároky z vadného plnění do pěti let od předání a převzetí Díla.

VI.
Ochrana informací

Zhotovitel nesmí nikomu zpřístupnit informace, které získal od Objednatele nebo od třetích osob v souvislosti s plněním této Smlouvy. Tyto informace jsou považovány za důvěrné a vztahuje se na ně dále sjednaná ochrana.

Za důvěrné informace jsou považovány veškeré informace poskytnuté Objednatelem nebo třetí osobou v souvislosti s plněním této Smlouvy v ústní nebo v písemné formě bez ohledu na jejich označení za důvěrné, zejména (i) veškeré poznatky obchodní, výrobní, technické či ekonomické povahy související s činností Objednatele nebo třetí osoby, které mají skutečnou nebo alespoň potenciální hodnotu a které nejsou v příslušných obchodních kruzích běžně dostupné a (ii) veškeré osobní údaje.

Ochrana důvěrných informací se nevztahuje na případy, kdy:

a) Zhotovitel prokáže, že je příslušná informace veřejně dostupná, aniž by tuto dostupnost způsobil sám Zhotovitel,

b) Zhotovitel prokáže, že měl tuto informaci k dispozici ještě před jejím zpřístupněním Objednatelem a že ji nenabyl v rozporu se svými právními povinnostmi,

c) Zhotovitel zpřístupní důvěrné informace za účelem plnění této Smlouvy členům svých orgánů, svým zaměstnancům nebo svým poddodavatelům, pokud jsou vázáni povinností mlčenlivosti nejméně v rozsahu vyplývajícím z této Smlouvy,

d) Zhotovitel zpřístupní důvěrné informace svým právním, ekonomickým nebo daňovým poradcům, pokud jsou tito vázáni povinností mlčenlivosti nejméně v rozsahu vyplývajícím z této Smlouvy,

e) Zhotovitel obdrží písemný souhlas Objednatele se zpřístupněním důvěrné informace, nebo,

f) je-li zpřístupněním důvěrné informace vyžadováno zákonem nebo závazným rozhodnutím oprávněného orgánu veřejné moci vydaným na základě zákona.

Zhotovitel se zavazuje nakládat s důvěrnými informacemi chráněnými dle této Smlouvy jako s obchodním tajemstvím; zavazuje se zejména uchovávat je v tajnosti a učinit veškerá smluvní a technická opatření zabraňující jejich zneužití či prozrazení.

Zhotovitel se zavazuje, že poučí členy svých orgánů, své zaměstnance a své poddodavatele, která, zpřístupní důvěrné informace, o povinnosti utajovat důvěrné informace v souladu s touto Smlouvou.

Jestliže důvěrné informace tvoří osobní údaje, je Zhotovitel dále povinen zabezpečit vhodnými technickými a organizačními opatřeními splnění všech povinností, plynoucích z právních předpisů upravujících ochranu osobních údajů, zejména pak z nařízení Evropského parlamentu a Rady (EU) 2016/679, obecného nařízení o ochraně osobních údajů, v platném znění, a ze zákona č. 110/2019 Sb., o zpracování osobních údajů, v platném znění.

Jestliže zhotovitel poruší kteroukoli ze svých povinností podle tohoto článku VI. této Smlouvy, zavazuje se Objednateli zaplatit smluvní pokutu ve výši 100.000,- Kč za každý případ porušení a nahradit škodu ve výši přesahující smluvní pokutu.

Povinnost utajovat důvěrné informace zavazuje Zhotovitele po dobu účinnosti této Smlouvy a po dobu pěti (5) let po předání a převzetí Díla.

VII.
Závěrečná ustanovení

Tato Smlouva nabývá platnosti dnem jejího podpisu oběma Smluvními stranami a účinnosti dnem jejího zveřejnění v Registru smluv.

Tato Smlouva a vztahy z ní vyplývající se řídí právním řádem České republiky, zejména příslušnými ustanoveními zák. č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

Smlouva byla vyhotovena ve dvou stejnopisech, z nichž každá Smluvní strana obdrží po jednom vyhotovení.

Obsah Smlouvy může být měněn jen dohodou stran smluvních a to vždy jen vzestupně číslovanými písemnými dodatky potvrzenými Oprávněnými osobami smluvních stran.

Smluvní strany níže svým podpisem stvrzují, že si Smlouvu před jejím podpisem přečetly, s jejím obsahem souhlasí, a tato je sepsána podle jejich pravé a skutečné vůle, srozumitelně a určitě, nikoli v tísni za nápadně nevýhodných podmínek.

Nedílnou součástí této Smlouvy jsou tyto přílohy:
- Příloha č. 1 Detailní popis testu
- Příloha č. 2 Ověřená kopie plné moci zástupce Zhotovitele

V Ústí nad Labem dne	V Teplicích dne
.....	.....
Objednatel	Zhotovitel
Dopravní podnik města Ústí nad Labem a.s.	**AUTOCONT a.s.**
Ing. Libor Turek, Ph.D.	Ing. Zdeněk Chobot
výkonný ředitel společnosti	ředitel regionálního centra, na základě plné moci

Příloha č. 1 – Detailní popis testu

1.1 Penetrační testy webové aplikace EOS

Penetrační test webové aplikace na produkční adrese https://eshop-bpk.dpmul.cz/.

Testy prověří aplikace z pohledu spolehlivosti, zajištění integrity a důvěrnosti dat. Testy jsou zaměřeny také na identifikaci bezpečnostních slabin, které se mohou vyskytovat v rámci instalace, konfigurace a procesů zpracování dat aplikace.

Součástí testů je také prověření bezpečnosti autentizačních a autorizačních mechanismů a způsobu zacházení s citlivými informacemi v rámci testovaných aplikací.

Penetrační testy aplikací zahrnují 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;
- pokus o získání přihlašovacích údajů registrovaného uživatele;
- bezpečnost technologií, na kterých jsou systémy postaveny (operační systémy, webové, aplikační a databázové servery) a jejich bezpečná integrace do zbývající infrastruktury;
- možnosti zneužití dostupných technologií v aplikaci útočníkem a proveditelné útoky na účty/relace legitimních klientů.

Při realizaci penetračních testů vycházíme z především z aktuální metodiky OWASP Testing Guide, přičemž používáme tyto níže uvedené techniky útoků a sběru informací.

Information Gathering

První fáze hodnocení bezpečnosti je zaměřená na sběr co největšího množství informací o cílové aplikaci. Sběr informací je nezbytný krok penetračního testování. S využitím volně dostupných nástrojů (vyhledávače, skenery, jednoduché odesílání HTTP dotazů, nebo speciálně upravené žádosti), je možné donutit aplikaci ke sdělení informací například ve formě chybových hlášení nebo oznámení verzí a používaných technologií.

Configuration and Deploy Management Testing

Analýza infrastruktury a architektura topologie často odkryjí zásadní informace o webové aplikaci. Také lze získat informace jako zdrojový kód, povolené http metody, administrační funkcionalitu, autentizační metody a informace o konfiguraci infrastruktury.

Identity Management Testing

Téměř každá moderní aplikace dnes disponuje mechanismem pro správu identit uživatelů, který se stará o proces zakládání a rušení uživatelů, správu rolí a proces identifikace uživatele v systému. V rámci prověrky budou testovány parametry tohoto mechanismu, identifikovány prohřešky proti best practice i chyby vedoucí k přímé kompromitaci zabezpečení aplikace.

Authentication Testing

Autentizace slouží pro ověření identity objektu či osoby. Příkladem procesu autentizace je běžné přihlášení uživatele k aplikaci. Testování schéma autentizace spočívá v analýze funkčnosti autentizačního procesu a pokusech o jeho obejití.

Authorization Testing

Autorizace je koncept povolení přístupu ke zdrojům pouze oprávněným uživatelům. Během těchto testů je zjišťováno, zda je možné obejití autorizačního schéma či nalezení cesty k eskalaci přidělených privilegií.

Session Management Testing

Session management je oblast zabývající se řízením stavu komunikace mezi webovým prohlížečem uživatele a webovou aplikací při použití bezestavových protokolů (HTTP). Při analýze této oblasti se zaměřujeme zejména na možnosti ukradení session, útoky typu man-in-the-middle a obdobné.

Data Validation Testing

Nejběžnější bezpečnostní slabinou webové aplikace je neschopnost aplikace ověřit vstupy přicházející od klienta nebo z prostředí před jejich použitím, zda obsahují předpokládané hodnoty a nikoliv škodlivý kód. Stejně tak je třeba ověřit korektnost výstupů, které aplikace poskytuje. Provedením této fáze je prozkoumána odolnost aplikace vůči útokům typu SQL/Code Injection, Cross-site scripting a dalším.

Error Handling Testing

Vyhodnocování nestandardních nebo chybových stavů a vytváření příslušných reakcí v podobě chybových hlášení a opravných akcí patří k běžným funkcím aplikací, bývá však velmi často spojeno s únikem citlivých informací nebo dokonce obejitím autorizačního schématu. Testy pomocí generování nestandardních vstupů jak do velikosti, tak obsahu slouží k detekci těchto chyb.

Cryptography Testing

Použití kryptografie k ochraně citlivých informací při přenosu nebo uložení citlivých dat bývá spojeno s celou řadou chyb, kterých se dopouštějí programátoři jak při návrhu mechanismu, tak i při jeho implementaci. Častým jevem bývá také použití nefunkčních nebo pro daný účel zcela nevhodných kryptografických mechanismů.

Business Logic Testing

Mimo vyloženě technicky zaměřených testů zkoumáme jednotlivá work flow obsažená v aplikaci a hledáme možnosti jejich zneužití k provedení aktivit, které nejsou v souladu se záměry vlastníka aplikace. Tyto testy se obvykle sestávají z následujících kroků:

- Pochopení aplikace.
- Vytvoření „syrových" dat pro návrh logických testů.
- Návrh logických testů.
- Naplnění předpokladů pro testování (jako např. vytvoření testovacích účtů s různými oprávněními).
- Provedení logických testů.

Client Side Testing

Tato kategorie testů má za úkol ověřit, jak účinné mechanismy aplikace používá proto, aby chránila své uživatele před specializovanými útoky, které směřují přímo na uživatele a jeho prohlížeč. Obvykle se jedná o různé druhy injekcí klientských skriptovacích jazyků a manipulaci s parametry spravovanými prohlížečem.

1.2 Penetrační testy mobilní aplikace EOS

Penetrační test mobilní aplikace EOS, napojené na produkční prostředí.

Součástí testů bude široké otestování zabezpečení komunikačního kanálu mezi mobilním klientem a webovým rozhraním https://eshop-bpk.dpmul.cz/. Analýza bude provedena na OS Android verze 8, 9 a 10 a iOS ve verzi 11, 12 a 13.

Penetrační testy představují simulaci napadení testovaných aplikací útočníkem. Jejich hlavním cílem je zjistit, jak snadný cíl tyto aplikace představují, jaké informace o nich lze získat a jak lze detekovat zranitelnosti, které mohou být zneužity k získání neautorizovaného přístupu k citlivým informacím. Při identifikovaném nálezu je popsáno jeho riziko a následně je navrženo odpovídající doporučení k jeho odstranění.

Penetrační testy mobilních aplikací budou realizovány na následujících platformách:

- Apple iOS,
- Google Android.

V průběhu penetračních testů jsou používány postupy, techniky a nástroje dostupné na internetu za účelem co nejvěrnější simulace pravděpodobného postupu útočníka. Metodika realizace testů naší společnosti vychází především z vlastní zkušenosti penetračních testerů a dále z metodiky OWASP Mobile Testing Guide, která je standardem pro testování bezpečnosti mobilních aplikací. Tento postup zajišťuje komplexní přístup k prověření všech oblastí bezpečnosti mobilní aplikace.

Dále jsou uvedeny oblasti, které představují jednotlivé kategorie podrobené penetračnímu testování. Každá kategorie obsahuje popis a tabulku, ve které jsou uvedeny konkrétní testované části. Všechny tyto kategorie dohromady představují komplexní pohled na bezpečnost testované mobilní aplikace.

M1: Improper Platform Usage

Velmi častým jevem je nesprávné zacházení s funkcemi konkrétních mobilních platforem či selhání používání bezpečnostních prvků platforem nebo specifických mobilních zařízení. Příkladem mohou být Android intents, požadavky na oprávnění, špatné užívání otisku prstu či databáze Keychain nebo nějakého jiného bezpečnostního prvku, který je součástí mobilního operačního systému.

M2: Insecure Data Storage

Tato kategorie zahrnuje nebezpečné ukládání soukromých dat či úniky privátních informací z různých zdrojů postranních kanálů. V ideálním případě by mobilní aplikace neměla na zařízení ukládat žádná data, která by mohla útočníkovi vyzradit citlivé informace, jako například autentizační údaje pro přihlášení k aplikaci. Pokud je nutné ukládat citlivá data na zařízení, musí být uložena na správném místě a v šifrovaném formátu.

M3: Insecure Communication

Komunikace klientské aplikace se serverovou částí musí být zabezpečena tak, aby zajišťovala důvěrnost a integritu přenášených informací. V této části je testována bezpečnost použitého komunikačního protokolu, především pak použití bezpečných verzí protokolu, silných šifrovacích algoritmů, délky použitých klíčů a kontrola validních klientských a serverových certifikátů.

Mobilní aplikace jsou většinou postaveny na architektuře klient-server. Častou implementační chybou je nedostatečná kontrola přijatých uživatelských vstupů na straně serveru. Tyto zranitelnosti vedou k útokům typu injection, kdy útočník dokáže získat pomocí modifikace zaslaných zpráv citlivé informace ze serveru (backendu) nebo způsobí jeho nedostupnost (DoS).

M4: Insecure Authentication

Tato kategorie zahrnuje všechny případy nesprávného ověřování koncového uživatele či špatného řízení uživatelských relací.

M5: Insecure Cryptography

Tato oblast se zaměřuje na testování bezpečnosti použitých kryptografických modulů. Kryptografické chyby lze rozdělit do dvou hlavních kategorií - špatná implementace při použití silných kryptografických knihoven a implementace vlastních kryptografických modulů. V obou případech dochází k obejití šifrovacích algoritmů, což vede k získání citlivých informací, které by měly být pomocí kryptografie chráněny před zraky útočníka.

M6: Insecure Authentication

Jedná se o kategorii, která zachycuje chyby v autorizaci, např. Rozhodnutí o autorizaci na straně klienta, enumerace zdrojů atd.

M7: Client Code Quality

Tento segment zachycuje všechny problémy s implementací mobilního klienta na úrovni kódu, např. překrývání vyrovnávacích pamětí, zranitelnosti formátovacího řetězce a různé další chyby na úrovni kódu, jejichž jediným řešením je přepsání některých částí kódu v mobilním zařízení.

M8: Code Tampering

Tato kategorie pokrývá terminologie jako binary patching, local resource modification, method hooking, method swizzling či dynamic memory modification. Jakmile je aplikace doručena do mobilního zařízení, jsou zde umístěny zdroje pro její kód a data. Útočník pak může buď přímo měnit kód, dynamicky měnit obsah paměti či změnit nebo nahradit systémové rozhraní API, které aplikace používá.

M9: Reverse Engineering

Tato kategorie zahrnuje možnosti binární analýzy aplikace, která umožňuje číst její zdrojový kód, knihovny, algoritmy a další assety. To může útočníkovi pomoci zneužít jiné, skryté, chyby v aplikaci, stejně tak jako odhalovat informace o aplikačních serverech, kryptografických konstantách a šifrách či duševním vlastnictví.

M10: Extraneous Functionality

Vývojáři do aplikací často vkládají skryté funkce, backdoory nebo jiné interní vývojářské bezpečnostní kontroly, které však nejsou určeny do produkčního prostředí. Příkladem může být zapomenuté heslo jako komentář v kódu hybridní aplikace.

M11: Business Testing

Kromě striktně technicky orientovaných testů zkoumáme jednotlivá work flow obsažená v aplikaci a hledáme možnosti jejich zneužití k provedení aktivit, které nejsou v souladu se záměry vlastníka aplikace. Tyto testy se obvykle skládají z následujících:

- pochopení aplikace,
- vytvoření "surových" dat pro návrh logických testů,
- návrh logických testů,
- implementace podmínek testování (např. vytváření testovacích účtů s různými oprávněními),
- provádění logických testů.

2 Průběh penetračních testů

2.1 Příprava

Před začátkem testů je potřeba zajistit nutné prerekvizity testu. Jedná se zpravidla o následující aktivity:

- ustanovení kontaktních osob;
- výběr prostředí (testovací, akceptační, produkční atd.),
- způsob provedení testů (vzdáleně nebo u zákazníka),
- zřízení vzdáleného přístupu k prostředí (VPN účty, povolení výjimek na náš adresní rozsah pro přístup přes Internet atd.),
- vytvoření a otestování přístupů do aplikací,
- zaslání dokumentace,
- způsob a formát reportingu (jazyk, šablona, průběžné informování o nálezech atd.),
- finální odsouhlasení termínů.

Délka trvání přípravné fáze je přibližně jeden týden a záleží především na schopnosti zákazníka připravit všechny podklady potřebné pro zahájení testů.

2.2 Testování

Veškeré testy se provádějí bez destruktivních zásahů (pokud je klient výslovně nepožaduje) tzn., že útok končí kompromitací systému, neprovádějí se žádné změny, které by poškodily informační systém.

Naše společnost používá k realizaci penetračních testů svoji vlastní metodiku, vyvinutou na základě zkušeností našich odborníků na informační bezpečnost, jež však zároveň vychází ze světově uznávaných standardů a zohledňuje i aktuální legislativu, která se týká bezpečnosti dat. Při penetračních testech vycházíme především z následujících metodik:

- OWASP (Open Web Application Security Project) – zaměřující se na pomoc organizacím při identifikaci bezpečnostních hrozeb především webových a mobilních aplikací.
  Penetrační testy provádíme především podle metodiky Testing Guide (případně MSTG pro mobilní aplikace). Na žádost zákazníka dokážeme testy provést podle metodiky Top Ten či ASVS (případně MASVS).
- PTES (The Penetration Testing Execution Standard) – technická doporučení pomáhající definovat postupy, které je třeba dodržet během penetračních testů.
- OSSTMM (Open Source Security Testing Methodology Manual) – metodologie pro testování bezpečnosti.
- NIST (National Institute of Standards and Technology) – především dokument 800-53 (CA-8) věnující se oblasti penetračních testů a red teamingu.
- CIS (Center for Internet Security) - nezisková entita, která se zaměřuje na ochranu soukromých a veřejných organizací před kybernetickými hrozbami.
- PCI-DSS (Payment Card Industry Data Security Standard) – pro splnění požadavku 11.3 daného standardu postupujeme dle Penetration Testing Guidance.
- CVE (Common Vulnerabilities and Exposures) – standardizovaný slovník obecných zranitelností a hrozeb.
- CVSS (Common Vulnerability Scoring System) – pro stanovení závažnosti dané zranitelnosti.

Bližší popis použitých metodik pro jednotlivé oblasti je uveden v odpovídajících kapitolách.

Na testech pracují vždy minimálně dva testeři, v případě malých projektů může být použit jeden seniorní tester. Délka trvání záleží na velikosti testovaného systému nebo aplikace. Vzhledem k šířce týmu naší společnosti trvají testy většinou jeden, maximálně dva týdny.

Konkrétní nástroje pro testování jsou vybírány operativně na základě provedených zjištění, a to takovým způsobem, aby pro daný systém či technologii byl použit vždy nejvhodnější (nejlépe zacílený) nástroj. Použití většího množství nástrojů také snižuje pravděpodobnost identifikace tzv. false positives, což jsou chybně detekované zranitelnosti testovaného systému. Pro minimalizaci těchto chybných nálezů jsou zranitelnosti prověřovány manuální metodou. Pravděpodobnost odhalení zranitelností je vysoká, umocněná dlouholetou zkušeností s penetračním a technickým testováním široké škály klientů a jejich systémů naší společností.

Následuje výčet několika základních nástrojů, používaných při penetračních testech:

- BurpSuite (http://portswigger.net/burp/)
- Netsparker (https://www.netsparker.com/)
- Nessus (http://www.tenable.com/products/nessus/nessus-product-overview)
- OpenVAS (http://www.openvas.org/)
- Arachni (http://www.arachni-scanner.com/)
- Metasploit (https://www.metasploit.com/)
- OWASP ZAP (https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project)
- Hydra (http:// thc.org/thc-hydra/)
- Netcat (http://www.l0pht.com/~weld/netcat/)
- Hping2 (http://www.kyuzz.org/antirez/hping2.html)
- Nmap (http://www.insecure.org/nmap/)
- Amap (http://www.thc.org/)
- Curl (http://curl.haxx.se/)
- Sslscan (http://sourceforge.net/projects/sslscan/)
- Vlastní skripty a další nástroje vyplývající z aktuální potřeby testovaného systému či aplikace

2.3 Závěrečná zpráva

Průběh penetračních testů a nalezené zranitelnosti jsou detailně sepsány do závěrečné zprávy, která je rozdělena na manažerské shrnutí a technickou část. Detailnější formát výsledné zprávy je popsán v kapitole **Chyba! Nenalezen zdroj odkazů.**. Zpráva je doručena v rámci několika dnů po dokončení testů, maximálně však do jednoho pracovního týdne.

Tento tzv. draft report je doručen v editovatelném formátu (MS Word) zákazníkovi, který má možnost ke zprávě připojit svoje komentáře. V případě požadavku může být seznam zranitelností doručen i v jiném formátu pro lepší strojové zpracování (MS Excel, CSV, …). Zranitelnosti je možné po domluvě reportovat přímo do ticketovacích systémů zákazníka (JIRA, Service Desk, GitHub, …).

Výstupem penetračních testů je závěrečná zpráva o stavu technické bezpečnosti prověřovaných systémů, která je rozdělena na část manažerského shrnutí (může být i samostatným dokumentem) a na detailní zprávu. Výstupy jsou standardně dodávány pomocí zašifrovaného archivu, uloženého na specializovaném webovém úložišti (v případě zájmu na CD/DVD) spolu s výstupy z použitých nástrojů a případnými doplňujícími informacemi k testům (např. screenshoty z průběhu testů).

Zpráva bude vypracována v českém jazyce.

Manažerské shrnutí

Pro účely managementu organizace je vypracována speciální hodnotící zpráva s cílem podchytit a stručně a srozumitelně popsat zjištěné výsledky testování a analýz.

Cílem manažerského shrnutí bude 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 technická zpráva

Obsahem detailní zprávy jsou konkrétní zjištění související s jednotlivými zkoumanými oblastmi. Detailní zpráva obsahuje 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.

Všechny identifikované zranitelnosti jsou popsány v následující struktuře:

Hodnocení/kategorizace zranitelnosti - veškeré nalezené problémy a zranitelnosti jsou rozděleny do pěti kategorií podle závažnosti.

CRITICAL	Kriticky závažné chyby (KRITICKÁ/CRITICAL) C Jako kritické chyby jsou označeny nedostatky, které byly při testech zneužity a vedly (mohou vést) k přímé kompromitaci testovaného systému.
HIGH	Závažné chyby (VYSOKÁ/HIGH) H Jako závažné klasifikujeme chyby, které bezprostředně umožňují kompromitaci systému, či jeho nedostupnost. U těchto chyb existuje velmi vysoká pravděpodobnost zneužití. Jejich okamžitá náprava je nutná.
MEDIUM	Středně závažné chyby (STŘEDNÍ/MEDIUM) M 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.
LOW	Méně závažné chyby (NÍZKÁ/LOW) L Tato kategorie zahrnuje méně závažné 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.
INFO	Informativní nálezy (INFORMATIVNÍ/INFO) I 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.

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.

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.

 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.
 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.

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

 HIGH	Pro odstranění zranitelnosti klasifikované tímto stupněm předpokládáme nutnost rozsáhlejších, strukturálních změn v kódu aplikace nebo její kompletní přepracování, nasazení nových technologií na úrovni infrastruktury nebo rozsáhlé změny infrastruktury.
 MEDIUM	Pro odstranění zranitelnosti klasifikované tímto stupněm odhadujeme, že pro vyřešení identifikovaných zranitelností bude potřeba udělat středně rozsáhlé změny v kódu aplikace, rozsáhlejší rekonfigurace serveru nebo související infrastruktury.
 LOW	Pro odstranění zranitelnosti klasifikované tímto stupněm odhadujeme náročnost implementace nápravných opatření v podobě úpravy konfiguračních parametrů aplikace nebo související infrastruktury.

Zjištění – popis zranitelného místa/nálezu včetně popisu kde a jakým způsobem byla zranitelnost identifikována.

Riziko – popis rizik plynoucích z možného zneužití zranitelného místa včetně možných scénářů zneužití (kdo a za jakých podmínek je možné zranitelnost zneužít a jaké jsou možné dopady tohoto zneužití), posouzení dopadu rizika na produkční prostředí.

Doporučení – doporučení vedoucí k odstranění nalezených nedostatků, případně návrhy na zvýšení bezpečnosti stávajících bezpečnostních mechanismů a opatření. Tato doporučení se mohou týkat procesních změn, konfigurace zařízení (hardening systémů), návrhu nových bezpečnostních mechanismů pro zvýšení stávající úrovně bezpečnosti, doporučení pro uživatelská PC pro zvýšení bezpečnosti atd.

Přílohy - výstupy z použitých nástrojů, důkazy apod.

2.4 Prezentace výsledků

V rámci dodávky nabízíme uspořádání závěrečného workshopu nad výsledky penetračních testů. Ze strany zákazníka by se měla zúčastnit osoba zodpovědná za IT bezpečnost, business vlastník testovaného systému či aplikace, osoby odpovědné za IT infrastrukturu a vývojáři, kteří budou implementovat daná opatření (interní vývoj či externí dodavatelé). Z tohoto workshopu mohou vzniknout další návrhy na změny v draft reportu, především v oblasti závažnosti nálezů či doporučených oprav.

2.5 Finální zpráva

Finální zpráva je zaslána ve formátu PDF po zapracování a odsouhlasení všech změn vzniklých z komentářů zákazníka, případně ze závěrečného workshopu. Zároveň se zprávou je zaslán k podpisu i akceptační protokol a případný požadavek na referenci.

2.6 Retesty

V rámci cenové nabídky je zahrnuto jedno kolo tzv. retestů, tedy kontroly vhodné implementace nápravných opatření na všechny nalezené zranitelnosti. Retesty závažných zranitelností mohou pro urychlení procesu probíhat již v průběhu testování. Zpravidla se však provádí do 3 měsíců od dodání finální zprávy.

Příloha č. 2 – Ověřená kopie plné moci zástupce Zhotovitele