SMLOUVA O POSKYTNUTÍ SLUŽBY PENETRAČNÍHO TESTOVÁNÍ

Město Dobříš, se sídlem Mírové náměstí 119, 263 01 Dobříš, IČO: 00242098, zastoupené Ing. Pavlem Svobodou, starostou města

(„**Objednatel**")

a

Integra Czech Republic, s.r.o., se sídlem U Sluncové 666/12a, Karlín, 186 00 Praha 8, IČO 24216941, Zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 189573, zastoupená Jiřím Harcubou, jednatelem

(„**Poskytovatel**")

Poskytovatel a Objednatel společně jako „**Smluvní strany**", nebo jednotlivě jako „**Smluvní strana**", uzavírají tímto tuto smlouvu o poskytnutí služby penetračního testování (dále jen „**Smlouva**") dle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník (dále jen „**Občanský zákoník**").

1 Úvodní ustanovení

1.1 Tato Smlouva stanoví podmínky poskytnutí služby penetračního testování provozované Objednatelem ze strany Poskytovatele, jak je blíže vymezena touto Smlouvou.

1.2 Součástí této Smlouvy je jako její příloha č. 1 nabídka Poskytovatele blíže vymezující předmět plnění služby dle této Smlouvy (dále jen „**Nabídka**"). V případě rozporu mezi textem Smlouvy a Nabídkou má přednost text Smlouvy.

2 Předmět Smlouvy

2.1 Poskytovatel se zavazuje za podmínek sjednaných touto Smlouvou:

- Provést penetrační testování v souladu s mezinárodními metodikami OSSTMM, OWASP, PTES a LPT, tj. testování zranitelnosti infrastruktury a IT systémů;
- vyhotovení závěrečné zprávy o provedení penetračního testu v českém jazyce;
- bližší popis průběhu poskytování služby penetračního testování včetně struktury závěrečné zprávy je uveden v Nabídce.

2.2 Pracovníci Poskytovatele podílející se na plnění služeb podle této Smlouvy budou specialisté splňující příslušné kvalifikační předpoklady.

2.3 Objednatel se zavazuje zaplatit cenu ve výši a dle podmínek dohodnutých v této Smlouvě.

2.4 Předmět plnění bude spolufinancován z dotačního projektu „Bezpečnost datového centra města Dobříš“, registrační číslo projektu: CZ.06.01.01/00/22_004/0000230, financovaného z IROP (dále jen „Projekt“).

2.5 Zhotovitel je povinen uvádět povinné prvky publicity podle podmínek strukturálních fondů EU na všech tištěných dokumentech vytvořených v souvislosti s předmětem koupě (nevztahuje se na interní účetní dokumentaci apod.). Tyto povinné prvky publicity sdělí a poskytne zhotoviteli na vyžádání Objednatel.

3 Termín a další podmínky plnění

3.1 Služba penetračního testování bude dokončeno do 30 dní od podepsání této smlouvy, pokud nebude zajištěna součinnost ze strany Objednatele, může se termín posunout.

4 Cena

4.1 Cena za služby penetračního testování včetně vypracování závěrečné zprávy se sjednává ve výši 94.500 Kč bez DPH, včetně DPH 21 % pak 114.345 Kč.

4.2 Poskytovatel je oprávněn vystavit fakturu za celou cenu služby po akceptaci projektu této Smlouvy, se splatností 20 dnů od jejího vystavení.

4.3 Faktury musí splňovat náležitosti daňového dokladu podle § 28 zákona č. 235/2004 Sb., o DPH, bude obsahovat číslo a název dotačního projektu (konkrétně bude uveden text ve znění: Projekt „Bezpečnost datového centra města Dobříš“, reg. č. CZ.06.01.01/00/22_004/0000230, je spolufinancován z Integrovaného regionálního operačního programu“).

4.4 Faktura musí být doručena do IS DS: pnxbx8u.

4.5 Platba faktury bude provedena bezhotovostním převodem na účet Poskytovatele uvedený ve faktuře. Za den platby se považuje den, ve kterém byla řádně fakturovaná částka odepsána z účtu Objednatele.

5 Součinnost Smluvních stran

5.1 Objednatel je povinen poskytnout potřebnou součinnost pro provedení služby penetračního testování.

6 Komunikace Smluvních stran

6.1 Smluvní strany budou komunikovat primárně elektronickou formou.

6.2 Kontaktními osobami Objednatele pro účely plnění této Smlouvy jsou:

Jméno	E-mail	Telefon
Kořínková Jitka	korinkova@mestodobris.cz, epodatelna@mestodobris.cz	318 533 312
Svajčík Radek	svajcik@mestodobris.cz	602 119 453

6.3 Kontaktními osobami Poskytovatele pro účely plnění této Smlouvy jsou:

Jméno	E-mail	Telefon
David Pícha	David.Picha@integra.cz	+420 604 200 062

7 Náhrada škody

7.1 Smluvní strany odpovídají za způsobenou škodu v rámci platných právních předpisů a Smlouvy. Smluvní strany budou předcházet riziku vzniku škod v souvislosti s plněním Smlouvy.

7.2 Žádná ze Smluvních stran neodpovídá za škodu způsobenou v důsledku chybných či nesprávných zadání nebo jakýchkoli jiných informací předaných druhou Smluvní stranou.

7.3 Na odpovědnost za škodu způsobenou při plnění Smlouvy se uplatní okolnosti vylučující odpovědnost dle Občanského zákoníku.

7.4 Smluvní strany sjednávají, že maximální výše náhrady škody vzniklé při plnění této Smlouvy je omezena do výše hodnoty plnění dle této Smlouvy.

8 Důvěrné informace

8.1 Pro účely této Smlouvy výraz „**Důvěrné informace**" znamená veškeré informace, zejména náklady a ceny (potenciální nebo skutečné); zákazníci; dodavatelé; technologie; technické, finanční a obchodní strategie, marketingové a propagační strategie; IT informace, vlastní metodologie a postupy a obchodní tajemství (bez ohledu na to, zda je či není patentovatelné), týkající se příslušné Smluvní strany, ať už ústní nebo písemné, uložené nebo přenášené jakýmkoli médiem, které jsou zpřístupněny druhé Smluvní straně, přímo nebo nepřímo, stejně jako všechny údaje, záznamy, poznámky, analýzy, kompilace, studií nebo jiných dokumentů získaných z, nebo jinak použitých a zveřejněných jako Důvěrné informace s výjimkou informací, které:

8.1.1 byly veřejně k dispozici v době takového zveřejnění, nebo následně se stanou veřejně dostupnými jinak, než v důsledku porušení povinností tohoto závazku důvěrnosti ze strany příslušné Smluvní strany;

8.1.2 byly k dispozici příslušné Smluvní straně jako veřejné před uzavřením této Smlouvy;

8.1.3 byly nezávisle vyvinuty příslušnou Smluvní stranou bez přístupu k Důvěrným informacím;

8.1.4 druhá smluvní strana dala ke zveřejnění takové Důvěrné informace souhlas.

8.2 Smluvní strany se zavazují k níže uvedenému:

8.2.1 zacházet s Důvěrnými informacemi jako se soukromými a přísně důvěrnými, a v případě neexistence předchozího písemného souhlasu od druhé Smluvní strany nezpřístupnit Důvěrné informace žádné třetí osobě, ledaže takové sdělení bylo předem dohodnuto s druhou Smluvní stranou (ať už písemně nebo ústně), nebo to od příslušné Smluvní strany budou oprávněně žádat závazné právní předpisy, správní orgán nebo příslušný soud. Takové zpřístupnění nebude považováno za porušení této

Smlouvy, nicméně i v tomto případě však musí být Objednatel informován před tímto zveřejněním;

8.2.2 používat Důvěrné informace výhradně za účelem plnění této Smlouvy;

8.2.3 nesmí kopírovat nebo reprodukovat jakoukoli část Důvěrné informace bez předchozího písemného souhlasu druhé Smluvní strany, pouze v míře přiměřeně a nezbytné k provedení služeb dle této Smlouvy;

8.2.4 informovat druhou Smluvní stranu o porušení jakékoliv výše uvedené povinnosti bez zbytečného prodlení,

8.2.5 zavázat své pracovníky, jakož i každou třetí osobu, které příslušná Smluvní strana zpřístupnila Důvěrné informace, k povinnosti ochrany Důvěrných informací alespoň v rozsahu odpovídajícím této Smlouvě.

8.3 Povinnosti Smluvních stran k ochraně Důvěrných informací trvá i po skončení této Smlouvy.

8.4 Poskytovatel uděluje Objednateli neodvolatelný souhlas zveřejnit plně nebo částečně závěrečnou zprávu a/nebo certifikát podle odst. 2.1 této Smlouvy.

9 Smluvní Pokuty

9.1 V případě prodlení Objednatele se zaplacením peněžité částky Poskytovateli je Objednatel povinen zaplatit smluvní pokutu ve výši 0,05% z dlužné částky za každý den prodlení.

9.2 V případě prodlení Poskytovatele s dodáním služby podle odst. 3.1 této Smlouvy je Poskytovatel povinen poskytnout Objednateli slevu z ceny služby (podle odst. 4.1 této Smlouvy) ve výši 0,05% za každý den prodlení.

9.3 Za každé porušení ustanovení o ochraně Důvěrných informacích dle čl. 8 této Smlouvy je porušující Smluvní strana povinna zaplatit druhé Smluvní straně smluvní pokutu ve výši 50.000 Kč.

9.4 Ustanoveními o smluvní pokutě není dotčeno právo na náhradu škody, uhrazená smluvní pokuta se však započte do náhrady škody.

10 Ukončení Smlouvy

10.1 Tato Smlouva může být ukončena

10.1.1 písemnou dohodou obou Smluvních stran;

10.1.2 odstoupením od Smlouvy v případě podstatného porušení povinností vyplývajících z této Smlouvy druhou Smluvní stranou, přičemž takové odstoupení nabývá účinnosti ihned po dni doručení písemného oznámení druhé Smluvní straně.

11 Rozhodné Právo, řešení sporů

11.1 Tato Smlouva a její výklad se řídí právním řádem České republiky.

11.2 Smluvní strany budou své případné spory řešit vždy smírem, ve vzájemné shodě. Všechny spory vznikající z této smlouvy a v souvislosti s ní budou řešit místně a věcně příslušené soudy ČR.

12 Závěrečná ustanovení

12.1 Veškeré změny v této Smlouvě musí být v písemné formě a podepsány oběma Smluvními stranami.

12.2 Pokud některé z ustanovení této Smlouvy je, nebo se stane neplatným nebo nevymahatelným, nebude to mít vliv na platnost a vymahatelnost ostatních ustanovení této Smlouvy a Smluvní strany se zavazují nahradit takové neplatné nebo nevymahatelné ustanovení novým, platným a vykonatelným ustanovením, které nejefektivnější pro obchodní záměr Smluvních stran.

12.3 Zhotovitel se zavazuje umožnit osobám oprávněným k výkonu kontroly projektu, z něhož je veřejná zakázka hrazena, provést kontrolu dokladů souvisejících s plněním zakázky, a to po dobu nejméně 10 let od ukončení financování díla způsobem, který je v souladu s platnými právními předpisy České republiky a Evropských společenství.

12.4 Zhotovitel je povinen minimálně do konce roku 2035 poskytovat požadované informace a dokumentaci související s realizací projektu, z něhož je Veřejná zakázka hrazena, zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost.

12.5 Zhotovitel se zavazuje k dodržování mezinárodních sankcí Evropské unie, přijatých v souvislosti s ruskou agresí na území Ukrajiny vůči Rusku a Bělorusku, zejména nařízení Rady EU č. 2022/576, nařízení Rady (EU) č. 269/2014 ve spojení s prováděcím nařízením Rady (EU) č. 2022/581, nařízení Rady (EU) č. 208/2014 a nařízení Rady (ES) č. 765/2006 nebo v jejich prospěch (dále jen „mezinárodní sankce EU“).

12.6 Smlouva je, v souladu s podmínkami zákona č. 134/2016 Sb., podepsána elektronicky.

12.7 Uzavření této smlouvy bylo schváleno dle čl. 3 odst. 1 směrnice Rady města Dobříše č. 1/2020, o zadávání veřejných zakázek malého rozsahu, v platném znění, starostou města.

12.8 Tato smlouva nabývá platnosti podpisem poslední ze smluvních stran a účinnosti zveřejněním v registru smluv. Zveřejnění zajistí objednatel.

Příloha: 1) Nabídka Poskytovatele

V Dobříši dne dle el. podpisu

za objednatele:

Ing. Pavel Svoboda
Digitální podpis:
13.02.2025 08:30

Ing. Pavel Svoboda
Starosta

za dodavatele:

Jiří Harcuba
Digitálně podepsal Jiří Harcuba
Datum: 2025.02.13 08:12:35 +01'00'

Jiří Harcuba
jednatel

INTEGRA

předkládá nabídku na:

Penetrační testy

Zákazník:	**Město Dobříš**
Projekt:	Penetrační testy
Dodavatel:	**Integra Czech Republic, s.r.o.** U Sluncové 666/12a 186 00 Praha
Vypracoval:	David Pícha david.picha@integra.cz
Datum vytvoření:	13.12.2024
Platnost do:	12.1.2025

Obsah

1 Představení dodavatele

Integra Czech Republic, s.r.o. je česká soukromá společnost, která úspěšně působí na trhu IT služeb a kybernetické bezpečnosti od roku 2012. Jsme lídrem v oblasti zajištění kapacit IT specialistů, kybernetické bezpečnosti a vývoje softwarových řešení na míru. Naší misí je pomáhat klientům dosáhnout jejich cílů v oblasti informačních technologií díky inovativním řešením, vysoce kvalifikovanému týmu a neustálému zlepšování našich služeb.

1.1 Identifikační údaje

Obchodní název	Integra Czech Republic, s.r.o.
Datum založení	9. 2. 2012
Sídlo společnosti	U Sluncové 666/12a, 186 00 Praha 8
Jednatel	Jiří Harcuba
Webové stránky	www.integra.cz
Kontaktní údaje	security@integra.cz, +420 214 214 602
IČ	24216941
DIČ	CZ24216941
Bankovní spojení	Komerční banka a.s.
Číslo účtu	107-7261940297/0100
Certifikace ISO	ISO 9001 & 27001
Obrat společnosti	Více než 480 mil Kč bez DPH

1.2 Informace o společnosti Integra

Integra dlouhodobě spolupracuje s více než 300 klienty, mezi kterými najdete přední mezinárodní korporace i inovativní start-upy. Naše služby jsou vyhledávány napříč různými odvětvími – od bankovnictví a finančnictví, přes pojišťovnictví, telekomunikace a logistiku, až po zdravotnictví a další průmyslové sektory.

Hlavní portfolio služeb:

- Kybernetická bezpečnost
- Body Leasing (outsourcing IT specialistů)
- Vývoj softwaru na míru
- Vzdělávání a školení v IT bezpečnosti

Mezi našimi zaměstnanci najdete elitní tým zkušených IT profesionálů, kteří jsou vždy připraveni poskytnout vám nejlepší podporu při překonávání bezpečnostních výzev, kterým se ve světě informačních technologií stále častěji vystavujete.

Jsme hrdými držiteli certifikací **ISO 9001 a ISO 27001**, které potvrzují naše závazky k dodržování nejvyšších standardů kvality a bezpečnosti ve všech aspektech naší činnosti. Certifikace ISO 9001 nám umožňuje neustále zlepšovat procesy a poskytovat služby, které odpovídají potřebám našich klientů. Certifikace ISO 27001 potvrzuje naši odbornou schopnost chránit citlivá data našich klientů a zajistit nejvyšší úroveň informační bezpečnosti.

Společnost Integra byla také několikrát oceněna v žebříčku **"Českých TOP 100 ICT společností"** v letech 2020, 2021, 2022 a 2023. Tato ocenění potvrzují naši pozici mezi předními hráči na trhu IT služeb v České republice.

2 Úvod

Velmi si vážíme příležitosti navrhnout a provést penetrační testy pro vaši organizaci. Naši specialisté v oblasti kybernetické bezpečnosti mají rozsáhlé zkušenosti, které byly ověřeny prostřednictvím úspěšných projektů a bezpečnostních testů pro přední klienty. Díky bohatému portfoliu referencí jsme schopni potvrdit naši odbornost a přinést skutečnou hodnotu v oblasti etického hackingu.

Přístup a metodologie:

- Naše unikátní metodika, která spojuje osvědčené mezinárodní standardy jako OWASP a OSSTMM, s našimi vlastními postupy, zaručuje vysokou úroveň ochrany a přesné identifikování zranitelností.
- Manuální testování je pro nás klíčové, protože přesně napodobuje reálné útoky a techniky, které používají skuteční útočníci. Automatizované nástroje používáme tam, kde to výrazně zvýší efektivitu testování, aniž bychom snížili jeho kvalitu.
- Díky kombinaci manuálních a automatizovaných přístupů dokážeme efektivně odhalit i složitější bezpečnostní mezery, které by mohly být jinak přehlédnuty.

Naše přidaná hodnota:

- **Konzultace s odborníky:** Po testování vám naši experti podrobně vysvětlí výsledky a poskytnou detailní přehled o průběhu testů.
- **Certifikát o provedení testu:** Po dokončení testování obdržíte certifikát, který potvrzuje, že vaše systémy byly důkladně prověřeny a splňují vysoké standardy kybernetické bezpečnosti.
- **Online test zranitelností:** Nabízíme možnost provést rychlý online sken zranitelností zcela zdarma, což vám poskytne první přehled o možných slabých místech vašich veřejných služeb. Tuto službu naleznete na našem webu: https://www.integra.cz/cs/online-sken-zranitelnosti/
- **Školení zaměstnanců:** Nabízíme také školení zaměřené na zvýšení povědomí o kybernetické bezpečnosti pro vaše zaměstnance, abyste minimalizovali rizika spojená s lidským faktorem

Tým našich bezpečnostních expertů

- Jsme jedním z největších poskytovatelů penetračních testů v České republice
- Máme dlouholeté zkušenosti v oblasti IT bezpečnosti a detailní znalost široké škály platforem a systémů
- Naši odborníci pravidelně procházejí školeními v oblasti IT bezpečnosti a etického hackingu, abychom drželi krok s nejnovějšími hrozbami a technikami
- Náš tým se pyšní mezinárodními certifikacemi uznávanými po celém světě
    - OSCP (Offensive Security Certified Professional)
    - CEH (Certified Ethical Hacker)
    - CHFI (Computer Hacking Forensic Investigator)
    - ECSA (EC-Council Certified Security Analyst)
    - eJPT (eLearnSecurity Junior Penetration Tester)
    - eCPPT (eLearnSecurity Certified Professional Penetration Tester)
    - eWPT (eLearnSecurity Web Application Penetration Tester)
    - OSWP (Offensive Security Wireless Professional)
    - CMPen (Certified Master in Penetration Testing)
    - AWS CSC-C01 (AWS Certified Security – Specialty)
    - AWS CLF-02 (AWS Certified Cloud Practitioner)

3 Cenová nabídka

Integra Czech Republic, s.r.o., U Sluncové 666/12a
IČO: 24216941 / DIČ: CZ24216941
Bank: Komerční banka a.s., bank number: 107-7333280217/0100, IBAN: CZ20 0100 0001 0773 3328 0217, SWIFT: KOMBCZPPXXX

Datum vystavení: 13.12.2024
Datum platnosti: 12.1.2025

Odběratel:
Město Dobříš
Mírové náměstí 119
Dobříš
Česká republika
CZ00242098

Kontaktní osoba:
Radek Svajčík

Vystavil:
David Pícha
david.picha@integra.cz
+420 604 200 062

Penetrační testy

Popis položky	Počet	Cena / jedn.	Sleva	Cena po slevě	Celkem
Penetrační testy infrastruktury	7 MD	15 000,00 Kč	10%	13 500,00 Kč	94 500,00 Kč

Uvedené ceny položek jsou bez DPH

Celkem:	94 500,00 Kč
Částka DPH:	19 845,00 Kč
Celkem vč. DPH:	114 345,00 Kč

4 Technický detail testů

V rámci zajištění vysoké úrovně kybernetické bezpečnosti a efektivity nově nasazených bezpečnostních technologií v infrastruktuře Města Dobříš navrhujeme provedení komplexních penetračních testů Vaší infrastruktury. Cílem těchto testů je prověřit účinnost stávajících ochranných opatření, identifikovat potenciální zranitelnosti, a ověřit schopnost systému reagovat na reálné bezpečnostní hrozby.

4.1 Infrastrukturní testy

Infrastrukturní testy slouží k důkladné analýze bezpečnosti systémů a jejich související infrastruktury. Testy zahrnují identifikaci operačních systémů a aktivních služeb s cílem detekovat slabiny, které by mohly útočníkovi umožnit neoprávněný přístup.

Naše infrastrukturní penetrační testy jsou prováděny podle metodiky **OSSTMM**, která zajišťuje komplexní a hloubkové testování informačních systémů. Výstupem je detailní přehled o identifikovaných zranitelnostech a potenciálních rizicích, který je následně využit pro implementaci nápravných opatření a zvýšení bezpečnostní úrovně.

4.1.1 Interní penetrační test

Interní penetrační testy simulují útok z perspektivy útočníka, který již prolomil perimetr a má přístup do vnitřní sítě. Testy hodnotí účinnost implementovaných bezpečnostních opatření a prověřují možnost eskalace oprávnění, až po získání administrátorského přístupu k citlivým systémům (root/domain admin).

Tímto způsobem získáváme komplexní přehled o rizicích spojených s přístupem přes VPN a efektivních opatřeních, která lze implementovat k ochraně firemní infrastruktury.

Hlavní testované oblasti při testech interní infrastruktury:

Information Gathering

Sběr informací z dostupných zdrojů, které by mohl útočník využít ve svůj prospěch. Může se jednat o informace, které o sobě dává vědět server ve svých hlavičkách, informace z DNS systému a podobně.

Port scanning

V rámci port scanningu dochází k nalezení otevřených TCP/UDP portů na testovaných IP adresách.

Service enumeration

Na otevřených portech dochází k identifikaci provozovaných služeb (foot printing) a jejich verzí.

Default credentials / weak password guessing

Pokud nalezená služba umožňuje autentizaci / autorizaci, je provedeno testování na výchozí přihlašovací údaje a proveden slovníkový útok (dictionary attack) na nejčastěji používaná / slabá hesla a účty.

Vulnerability scanning

Na základě zjištěných verzí služeb dochází k porovnání se seznamem známých zranitelností (http://www.cvedetails.com/, http://www.securityfocus.com/, https://www.exploit-db.com/)

Exploitation

Pokud je nalezena zranitelná služba, je provedena její exploitace a získání přímého přístupu (shell) k testovanému cíli.

Privilege escalation:

Zvýšení úrovně oprávnění získaného přístupu k maximální možné úrovni (root/administrator).

Post-exploitation

Po získání přímého přístupu k testovanému cíli dochází k prohloubení penetrace a rozšíření přístupu v rámci daného systému/sítě.

Lateral movement:

Prozkoumání sítě a nalezení dalších zranitelných systémů.

Data exfiltration:

Odcizení citlivých dat z testovaného systému.

4.1.2 Externí penetrační test

Externí penetrační test simuluje kybernetický útok na komponenty informačního systému organizace z perspektivy externího útočníka. Cílem tohoto testu je důkladně posoudit odolnost ICT infrastruktury a identifikovat potenciální bezpečnostní rizika. Test odhaluje slabiny, které by mohly být zneužity k neoprávněnému přístupu nebo poškození systémů.

Hlavní testované oblasti při testech z veřejné sítě:

Information Gathering:

Získání dostupných dat, která by mohla být využita útočníkem. To zahrnuje analýzu informací z DNS systémů, serverových hlaviček a dalších veřejně dostupných zdrojů. Tento krok je klíčový pro identifikaci možných vstupních bodů do systému.

Port Scanning:

Identifikace otevřených TCP/UDP portů na testovaných IP adresách. Tato fáze umožňuje mapovat síť a pochopit, jaké služby jsou dostupné pro útok.

Service Enumeration:

Na nalezených otevřených portech se provádí detailní identifikace spuštěných služeb a jejich verzí. Tento krok pomáhá odhalit zranitelnosti specifické pro jednotlivé služby.

Default Credentials / Weak Password Guessing:

Pokud nalezená služba umožňuje autentizaci nebo autorizaci, provádíme testování na výchozí přihlašovací údaje a provádíme slovníkový útok (dictionary attack) na běžně používaná a slabá hesla. Tímto způsobem můžeme zjistit, zda jsou implementovány silné autentizační postupy.

Vulnerability Scanning:

Porovnání detekovaných verzí služeb s databázemi známých zranitelností (např. CVE, Exploit-DB). Tato analýza odhaluje potenciální slabiny, které by mohly být zneužity útočníky.

Exploitation:

Pokud je nalezena zranitelná služba, provádíme exploitaci. Využíváme různé techniky pro získání přístupu k cílovému systému, například získání shellu. Tato fáze nám umožňuje potvrdit, jak hluboko může útočník proniknout do systému a jaké škody může napáchat.

Post-Exploitation:

Po úspěšné exploitaci se zaměřujeme na rozšíření přístupu v rámci systému, identifikaci dalších cenných cílů a zachycení citlivých dat. Tato fáze nám pomáhá pochopit, jak útočník může dále manipulovat s dostupnými systémy.

Privilege Escalation:

Analýza způsobů, jakými může útočník zvýšit úroveň svých oprávnění na maximální možnou úroveň (např. root nebo administrátor). Tento proces zahrnuje hledání zranitelností a slabých míst, které umožňují eskalaci práv.

5 Testování

V průběhu testování využíváme kombinaci manuálních a automatizovaných metod, přičemž zohledňujeme povahu testovaných systémů a aplikací. Pokud jsou testy prováděny v produkčním prostředí, minimalizujeme použití automatizovaných testů a zásahů do systému, aby bylo zajištěno co nejmenší riziko pro funkčnost testovaných aplikací a systémů.

Na základě analýzy Vašich systémů a požadavků vypracujeme konkrétní plán penetračního testu, který bude odpovídat charakteristice testovaných technologií. Následně použijeme specializované nástroje a techniky pro identifikaci zranitelností. Mezi naše běžně používané nástroje patří: Nmap, Nikto, MetaSploit, Burp Suite, Nessus, OWASP ZAP, Hydra, Aircrack-ng, Gophish a mnoho dalších.

S pomocí těchto nástrojů identifikujeme zranitelnosti testované platformy a následně vytváříme a upravujeme skripty pro jejich exploitaci.

5.1 Výsledky a vyhodnocení

Po dokončení testování obdržíte podrobný report, který obsahuje detailní popis metod testování, nástrojů a všech identifikovaných zranitelností. Každé nalezené slabé místo je hodnoceno podle CVSS klasifikace, což umožňuje stanovit jeho závažnost.

Struktura závěrečné zprávy je následující:

A) Manažerské shrnutí

- Stručně a přehledně shrnuje hlavní výsledky testování, včetně nalezených bezpečnostních rizik, jejich závažnosti a doporučených opatření pro jejich eliminaci.

B) Technická zpráva

- Cíle a rozsah testování
- Popis provedených testů a použitých metod
- Vysvětlení klasifikace zranitelností
- Podrobný přehled výsledků z každé fáze testování
- Seznam všech nalezených zranitelností a doporučení pro jejich odstranění
- Závěrečné zhodnocení provedeného testu

5.2 Harmonogram

Následující harmonogram vychází z našeho předpokládaného průběhu prací. Pokud máte jiná přání ohledně termínu realizace, prosím informujte nás, abychom se mohli pokusit vyjít vstříc vašim preferencím.

Na samotné testování aktuálně plánujeme kapacity minimálně 20 pracovních dní dopředu.

Dokončení	Fáze	Popis a poznámky	Délka trvání
T + 0	**Kick-off meeting**	Zahajovací schůzka k upřesnění rozsahu, cílů a časového rámce. Vydefinování potřebné součinnosti ze strany zadavatele	1 den
T + 20	**Zajištění součinnosti**	Klient poskytne přístupy, seznam IP, domén či jiné potřebné podklady dle specifikace z kick-offu	1-20 dní
T + 28	**Testování**	Aktivní provádění penetračních testů. Průběžná komunikace o kritických nálezech	8 dní
T + 32	**Vypracování reportu**	Tvorba zprávy (technická + manažerská část) s doporučeními. Přizpůsobení specifikům klienta	2–4 dny
T + 33	**Prezentace výsledků**	Předání reportu elektronickou formou, případná diskuse o zjištěních a návrh dalších kroků	1 den

5.3 Potenciální rizika spojená s penetračními testy

Primárním cílem penetračních testů je identifikace bezpečnostních zranitelností v sítích, systémech nebo aplikacích („testovaný objekt“). Aby bylo možné tyto zranitelnosti spolehlivě detekovat, je často nutné komunikovat a interagovat s testovaným objektem jinak než běžným způsobem uživatelské interakce. I když je testování prováděno zkušeným bezpečnostním odborníkem s náležitou péčí, je přesto možné neúmyslně způsobit poškození testovaného objektu. Ve vzácných případech může dojít k úpravě nebo smazání dat, výpadku nebo poruše testovaného objektu, připojených systémů a obchodních procesů. Příklady zahrnují mimo jiné:

- Shromažďování informací o struktuře aplikace nebo běžících síťových službách může vést k výpadku nebo poruše testovaného objektu a/nebo připojených systémů.
- Exploitace identifikované zranitelnosti může vést k výpadku nebo poruše testovaného objektu a/nebo připojených systémů.
- Exploitace identifikované zranitelnosti může způsobit změnu nebo smazání dat.
- Nepřímo či přímo připojené systémy mohou vytvářet záznamy v logu nebo alarmové zprávy, které mohou ovlivnit další systémy nebo procesy.

Denial of Service (DoS) – Obecně nejsou používány žádné metody nebo techniky, které by záměrně narušily testovaný objekt nebo připojené systémy (Denial of Service). Rovněž se vyhýbáme metodám nebo technikám, které by mohly smazat nebo změnit data zpracovaná nebo uložená.

Zálohy – Je nezbytné, aby před zahájením byli vytvořeny zálohy potřebné k obnově dat nebo testovaného objektu.

Kontaktní osoba – Po dobu testování by měly být všechny osoby zapojené do správy testovaného objektu informovány o probíhajícím hodnocení. Měla by být určena kontaktní osoba, kterou bude možné kontaktovat v případě problémů.

Služby třetích stran / Cloudová prostředí – Pokud smlouva o úrovni služeb vyžaduje schválení od třetí strany před provedením penetračního testu, klient si musí zajistit schválení od třetí strany (např. poskytovatele hostingu nebo cloudových služeb) před zahájením hodnocení.

Samostatné testovací prostředí – Vzhledem k povaze a záměru penetračních testů může testování v produkčním prostředí ovlivnit provozní činnosti systému. Aby se předešlo narušení, doporučuje se použít samostatné prostředí pro testování, které je identické s produkčním prostředím, místo produkčního prostředí.

Prohlášení klienta

- Jsme obeznámeny s tím, že testování může způsobit poruchu nebo výpadek testovaného objektu či připojených systémů nebo ztrátu dat.
- Potvrzujeme, že všechny strany zapojené do testovaného systému (např. poskytovatelé hostingu nebo cloudových služeb) byly informovány a vydali potřebná povolení.
- Přijetím této nabídky povolujeme poskytovateli penetračních testů provést penetrační test.

6 Reference

Klient		Typ penetračních testů
Home Credit international	HOME CREDIT	API, Web aplikace, Mobilní aplikace, Interní infrastruktura, Externí infrastruktura, Baiting, Phishing
LOGEX	LOGEX HEALTHCARE ANALYTICS	API, Web aplikace, Mobilní aplikace, Interní infrastruktura, Externí infrastruktura
Partners Bank	Partners Banka	API, Web aplikace, Mobilní aplikace
Afriland First Bank	Afriland First Bank	Web aplikace, Externí infrastruktura
Wultra	wultra	API, Web aplikace, Mobilní aplikace
NumberFour AG	enfore	API, Web aplikace, Externí infrastruktura, AWS
Allianz	Allianz	API, Web aplikace, Mobilní aplikace, Interní infrastruktura, Externí infrastruktura
Česká Spořitelna	ČESKÁ spořitelna	API, Web aplikace, Mobilní aplikace, Interní infrastruktura
Schwarz Gruppe	SCHWARZ, LIDL, Kaufland	API, Web aplikace, Mobilní aplikace, Interní infrastruktura, Externí infrastruktura
ŠKODA ICT	ŠKODA	API, Web aplikace, Interní infrastruktura
UCED	UCED	Web aplikace, Interní infrastruktura, Externí infrastruktura, Phishing, Vishing
SIEMENS	SIEMENS	Interní infrastruktura, Externí infrastruktura

** Větší detail testů zde záměrně neuvádíme, bohužel ne vždy jej můžeme nasdílet*

7 Realizační tým

Penetrační testeři	**Certifikace**	**Jazyk**
Josef Havel	CHFI, CEH, ECSA, eWPT	CZ / EN
Michal Frič	CEH Master	CZ / EN
Elena Selkina	CompTIA Security+	CZ / EN / RU
Timotei Adamec	eJPT, eCPPT, eWPT, CMPen, AWS CLF-C02	CZ / EN
Filip Phouc anh Tran Huu	PNTP	CZ / EN / VIET
František Kotačka	OSCP, SCS-C01 AWS	CZ / EN
Marek Murgaš	OSCP, KLCP, OSWP	SK / EN
Projektový tým	**Role**	**Jazyk**
David Pícha	Vedoucí oddělení Security	CZ / EN
Adrian Šrajer	Cyber Security BDM	CZ / EN / DE
Kateřina Csirková	Projektová manažerka	CZ / EN

8 Závěr a poděkování

Vážíme si příležitosti poskytnout Vám naše profesionální služby v oblasti penetračních testů. Kybernetická bezpečnost je dnes klíčovým tématem a s rostoucí složitostí IT systémů je nezbytné identifikovat a eliminovat potenciální zranitelnosti.

Penetrační testování je pro nás posláním – nejen službou, ale i cestou, jak pomoci organizacím chránit jejich data a systémy. Naši klienti oceňují detailní provedení testů a konkrétní ukázky exploitace, které jasně ukazují závažnost nalezených zranitelností.

Děkujeme za Vaši důvěru a těšíme se na úspěšnou spolupráci.