Řešení informační bezpečnosti

Specifikace nabídky

Předkládá
Aricoma Enterprise Cybersecurity a.s.
Voctářova 2500/20a, Libeň (Praha 8), 180 00
Praha IČO: 04772148, DIČ: CZ04772148

Vypracoval
[redacted]

Datum vytvoření: 09. 04. 2025

Platnost do: 30. 04. 2025

Vypracováno pro:

Správa Železnic

ARICOMA

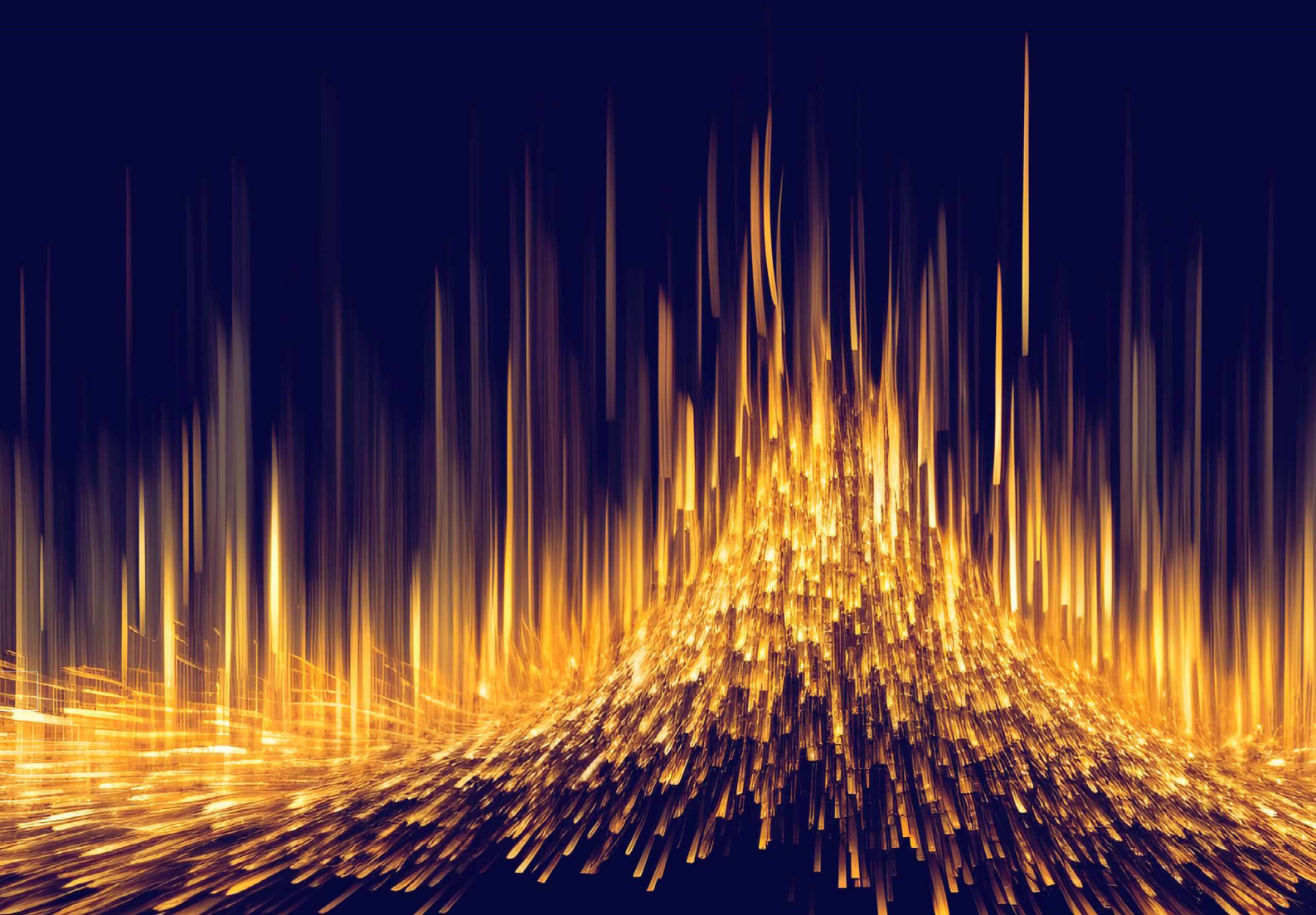
ARICOMA

O společnosti

Aricoma poskytuje služby v oblasti IT infrastruktury, cloudových technologií, podnikových aplikací, kybernetické bezpečnosti, digitalizace veřejného sektoru a systémové integrace. Firma stojí na pevných základech více než třicetileté historie poskytování služeb v oblasti ICT. Za úspěšným rozvojem stojí umění lidí vhodně reagovat na nové trendy a inovace. Značku Aricoma tvoří profesionálové s plnou důvěrou a autonomií.

Spolupracujeme s předními světovými dodavateli technologií a zákazníkům umíme nezávisle nabídnout pro ně to nejvhodnější řešení. Každý den je provádíme světem digitální transformace.

Máme jasnou vizi o budoucnosti oboru a našeho podnikání: Chceme dále rozvíjet naše služby v České republice a na Slovensku, výrazně posílit spolupráci s institucemi a úřady Evropské unie a stát se preferovaným poskytovatelem ICT služeb v německy mluvících zemích.



Obsah

1. Základní údaje o uchazeči

Obchodní jméno	Aricoma Enterprise Cybersecurity a.s.
Právní forma	akciová společnost
Rok založení	1991
Sídlo společnosti	Voctářova 2500/20a, 180 00 Praha
Adresa kanceláře	Voctářova 2500/20a, 180 00 Praha
Seznam statutárních zástupců	Jiří Bíba, Předseda představenstva Michal Tománek, Místopředseda představenstva Tomáš Strýček, člen představenstva Tomáš Ječmínek, Člen představenstva David Emr, Člen představenstva
Kontaktní údaje	Tel.: +420 226 229 133 www.aricoma.com
IČO	04772148
DIČ	CZ04772148
Zápis v OR	Společnost je zapsána v Obchodním rejstříku vedeném Městským soudem v Praze, spisová značka B 21326
Výpis z OR, ŽR a RT	Výpisy z Obchodního rejstříku, z Rejstříku trestů a Výpis z veřejné části Živnostenského rejstříku jsou přiloženy v samostatných PDF dokumentech
Bankovní spojení	Česká spořitelna a.s.
Číslo účtu	[redacted]
Zástupce v tomto jednání	[redacted]

1.1 Technologičtí partneři

Jako bezpečnostní expert Aricoma Enterprise Cybersecurity pomáhá svým klientům řešit náročné bezpečnostní problémy a orientovat se v nových produktech a technologiích. V současné době úzce spolupracujeme se společnostmi RSA, Forcepoint, CyberArk, Check Point a F5 - lídry v oblasti prevence ztráty dat (DLP), monitorování SIEM, správy privilegovaných účtů (PAM), firewallů či firewallů webových aplikací (WAF).

1.2 Představení divize Security Assessment

Zkušenosti našich Cyber Security specialistů jsou prověřeny a ověřeny řadou realizovaných testů bezpečnosti a dalších projektů v oblasti ICT bezpečnosti, které jsme realizovali především v oblasti finančních institucí, což dokládáme mj. přiloženými referencemi.

Mezi naše hlavní přednosti, které můžeme jako dlouhodobý partner v oblasti penetračních testů poskytnout, patří zejména:

Tým specialistů a konzultantů

- Disponujeme největším týmem etických hackerů v České a Slovenské republice, který má aktuálně 16 členů.
- Široká základna specialistů umožňuje pracovat jak na velkých projektech, tak i na malých úkolech, realizovaných v rámci několika dní.
- Navržený tým pro realizaci penetračních testů nasbíral bohaté zkušenosti z prověrek informačních systémů a infrastruktury předních českých i zahraničních společností.
- Všichni členové týmu jsou prověření kmenoví zaměstnanci, nevyužíváme žádné kontraktory.
- Vybraní specialisté drží certifikace CISSP, OSCP, OSWP, CISA, eMAPT, C|EH a další.

Metodika a přístup

- Předmětem nabídky je komplexní prověrka dle metodiky Aricoma Enterprise Cybersecurity pro testování aplikací a infrastruktury, která především vychází z metodik OWASP, PTES a OSSTMM a rozšiřuje je o interní postupy Aricoma Enterprise Cybersecurity.
- Při penetračních testech nespoléháme jen na automatizované nástroje, ale upřednostňujeme ruční testování, které více simuluje činnost útočníka. Naší specialitou je pak testování business logiky aplikací, která vyžaduje hluboké znalosti a zkušenosti s finančně orientovanými aplikacemi.

- Součástí výstupů projektu je i závěrečné zhodnocení bezpečnosti testované aplikace formou manažerského shrnutí. Každá zranitelnost je pak kategorizována z pohledu závažnosti, pravděpodobnosti zneužití a náročnosti odstranění.

Zkušenosti a reference

- Využití dlouholetých zkušeností Aricoma Enterprise Cybersecurity s penetračními a technickými testy, bezpečnostními audity a souvisejícími aktivitami jako jsou analýzy rizik, návrh bezpečné infrastruktury, vytváření bezpečnostní dokumentace, tvorba havarijních plánů a plánů kontinuity apod.
- Znalost bankovního prostředí a finančních aplikací téměř všech významných institucí pohybujících se na Českém a Slovenském trhu i zkušenosti se zahraničními pobočkami finančních institucí.
- Jako jedna z mála společností v Evropě se můžeme pochlubit certifikací a schválením realizovat penetrační testy v mezinárodní skupině Raiffeisen.
- Důkazem naší kvalifikace a zkušeností jsou přiložené referenční zakázky.

2. Popis nabídky

Předmětem této nabídky jsou penetrační testy infrastruktury Správy Železnic. Dle dohody budou detaily upřesněny po podpisu NDA.

2.1 Penetrační testy externí infrastruktury

Vnější penetrační test představuje simulaci napadení komponent informačního systému útočníkem z vnějšího prostředí. Cílem testů je zjistit, jak snadno identifikovatelný cíl ICT infrastruktura organizace představuje, jaké informace lze získat o zvenčí dostupných komponentách, jak detekovat zranitelnosti, které mohou být zneužity k získání neautorizovaného přístupu k citlivým systémovým zdrojům, a navrhnout doporučení k jejich odstranění. Testy budou vedeny z testovacího prostředí Aricoma přes internet.

V následujících odstavcích jsou uvedeny obecné činnosti, jejichž cílem je získat podklady pro komplexní hodnocení bezpečnosti testovaných aplikací při penetračním testování.

Identifikace cíle

Základním předpokladem úspěšně provedeného útoku je dostatečná znalost cíle. V první fázi se pokoušíme určit, jak je obtížné identifikovat cílový systém dostupný z internetu (DNS jména, IP adresy). V rámci této fáze provádíme sběr dostupných informací (evidenční databáze, DNS, trasování, odezvy apod.).

Identifikace aktivních služeb

Provádíme skenování portů, kdy se připojujeme přímo k jednotlivým TCP a UDP portům aplikace. Identifikace otevřených portů umožňuje zjistit s určitou jistotou typ např. operačního systému. V této fázi se využívají některé systémové nástroje a skenery portů.

Identifikace zranitelností

Na základě výsledků předchozí fáze a pomocí dalšího skenování aplikace provádíme zjišťování existujících zranitelností a výběr těch, které mohou být potencionálně zneužity k její kompromitaci. V této fázi se využívají skenery zranitelností a vlastní testovací sada nástrojů společnosti Aricoma.

Získání přístupu

S využitím nalezených zranitelností a dalších informací zjištěných v předchozích fázích se snažíme manuálně proniknout do aplikace/systému, případně získat další citlivé informace (např. uživatelská hesla). V případě, že je to možné, využívají se v této fázi nástroje pro „hádání“ hesel.

Eskalace privilegií a ovládnutí cíle

Cílem této fáze je získání plné kontroly nad aplikací (např. získání práva uživatele administrátor/root), identifikace možnosti instalace dalších aplikací (např. pro vzdálené ovládání cíle), případně identifikace možnosti využití aplikace k útoku a průnikům do dalších aplikací zadavatele.

Reakce na testy

V rámci této fáze jsou analyzovány případné reakce ochranných nástrojů zadavatele směřující proti prováděným testům (např. reakce IPS, administrátorů apod.).

2.2 Penetrační testy interní infrastruktury

Vnitřní penetrační test představuje simulaci napadení komponent informačního systému útočníkem z vnitřního prostředí společnosti. Cílem testů je zjistit, jak snadno identifikovatelný cíl ICT infrastruktura organizace představuje,

jak snadno lze detekovat zranitelnosti, které mohou být zneužity k získání neautorizovaného přístupu k citlivým systémovým zdrojům, a navrhnout doporučení k jejich odstranění. Testy budou vedeny z vnitřního prostředí společnosti. V rámci těchto testů jsou použity klasické zaměstnanecké přístupy (zpravidla doménové účty).

V následujících odstavcích jsou uvedeny obecné činnosti, jejichž cílem je získat podklady pro komplexní hodnocení bezpečnosti testovaných systémů při interních penetračních testech. Některé z fází na sobě nezávislé a mohou probíhat paralelně.

Identifikace prostředí a hledání zranitelností

První fáze zahrnuje rozpoznání a mapování jednotlivých systémů (typy serverů, operačních systémů atd.) a služeb dostupných v uživatelské síti organizace souvisejících s testovanými aplikacemi.

Testování bezpečnostních slabin souvisejících se softwarovými chybami, chybami v konfiguraci a chybami vycházejícími z nevhodného designu služeb.

Identifikace aktivních síťových prvků a prověření jejich bezpečnosti

Fáze zahrnuje rozpoznání aktivních síťových prvků jako firewall, gateway, síťové přepínače, směrovače a prověření jejich úrovně bezpečnosti z pohledu celkové koncepce sítě organizace, i z pohledu samotných systémů.

Testy budou realizovány automatizovanými metodami skenování, které rozpoznají strukturu sítě a vlastní zranitelnosti jednotlivých systémů dle získaných „otisků“ služeb. Dopady na bezpečnost sítě budou následně vyhodnoceny dle doporučení výrobců a uznávaných best practices.

Pokus o prolomení vybraných identifikovaných systémů a služeb – eskalace privilegií

Na základě výsledků předchozí fáze budou identifikovány a ověřeny možnosti povýšení daných práv a případného plného ovládnutí testovaných systémů zadavatele.

Jednotlivé testy budou realizovány různými metodami. Zejména však útoky hádání hesel, zneužití nalezených informací (nalezená hesla, skripty) a dále pak (v případě souhlasu zadavatele) i využití exploitů pro konkrétní nalezené zranitelnosti.

Pokus o kompromitaci domény společnosti

V této fázi bude uskutečněn pokus o eskalaci privilegií na úroveň doménového administrátora. Cílem této fáze je kompromitace interní domény společnosti. Během této fáze jsou použitý klasické i nejmodernější způsoby útočníků jakými jsou například Pass the Hash, LSASS Dumping, Incognito Token Impersonation a další.

3. Průběh penetračních testů

3.1 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 Aricoma Enterprise Cybersecurity 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.

3.2 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.

Aricoma Enterprise Cybersecurity 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 společnosti Aricoma Enterprise Cybersecurity 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

3.3 Závěrečná zpráva

Průběh penetračních testů a nalezené zranitelnosti jsou detailně sepsány do závěrečné zprávy, která je rozdělena na manažerské shrnutí a technickou část. 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 může být vypracována v českém nebo anglickém 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.

	**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.
	**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.
	**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.

3.4 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.

3.5 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.

3.6 Retesty

V rámci cenové nabídky je volitelně zahrnuto jedno kolo tzv. retestů, tedy kontroly vhodné implementace nápravných opatření na všechny nalezené zranitelnosti.

Podmínky pro provádění retestů

Objednání a provedení retestů: Retesty (opakované testování) mohou být provedeny pouze v rámci 3 měsíců od data dokončení původního testování, pokud jsou objednány zároveň s hlavním testováním nebo při jeho uzavření.

Dodatečné objednání retestů: Pokud budou retesty objednány později než při uzavření smlouvy na hlavní testování, může být jejich provedení odmítnuto nebo účtováno dle aktuálního ceníku, který se může lišit od původní cenové nabídky.

Infrastruktura pro retesty: Retesty budou provedeny na stejné infrastruktuře jako původní testování. Pokud zákazník požaduje provedení retestů na jiné infrastruktuře, je nutné to specifikovat již při objednávce, jinak nebude garantována konzistence výsledků.

4. Harmonogram

Níže uvádíme orientační harmonogram činností. Termíny mohou být po vzájemné dohodě upraveny.

Fáze projektu	Termín realizace
Příprava testů	4 / 2025
Penetrační testy	4 / 2025
Zaslání finální zprávy a akceptace testů	4 / 2025

Uvedený časový harmonogram i cenová nabídka je platná pro režim dodávky ve standardních pracovních hodinách: Po-Pá, 8:00 – 18:00. Plnění mimo toto časové rozmezí je možné po dohodě.

5. Cenové a platební podmínky

5.1 Platební podmínky

Platba za předmět plnění (provedení bezpečnostních testů) bude provedena na základě faktury vystavené do 14 dnů od předání výstupů jednotlivých aktivit. Splatnost těchto faktur je 30 dnů.

5.2 Záruční doba (na cenu a termín dodávky)

Cena je v kontextu této nabídky stanovená jako nepřekročitelná, platná po celou dobu realizace díla. V případě, že v průběhu testovací fáze dojde k jakékoliv změně zadání či rozšíření specifikace nebo rozsahu testování, které by bylo odlišné od původně specifikovaných požadavků, společnost Aricoma Enterprise Cybersecurity a.s. o této změně písemně informuje klienta prostřednictvím elektronické pošty. Následně se obě strany dohodnou na odpovídající úpravě ceny.

5.3 Součinnost a závaznost domluveného termínu

V případě potvrzení a následného zrušení dohodnutého termínu služby ze strany zákazníka v období kratším než deset pracovních dnů před plánovaným zahájením služby, nebo v případě, že nebude klient schopen poskytnout nezbytnou spolupráci pro zajištění poskytnutí služby naší společností, vzniká klientovi povinnost uhradit naší společnosti částku rovnající se 25 % z celkové hodnoty objednané služby bez DPH.

5.4 Cenový návrh

Cena za ManDay (MD) práce specialistů je stanovena na 14 800,- Kč bez DPH.

Aktivita	MD	Cen bez DPH
Penetrační testy infrastruktury	8	118 400 Kč
Projektový Management + Reporting	1	14 800 Kč
Re-testy	1	14 800 Kč
Celkem*		**148 000 Kč**

*Pokud během testování zjistíme skutečnosti, které nebyli v zadání, může se počet MD změnit.

6. Závěr

Všichni pracovníci společnosti Aricoma Enterprise Cybersecurity a.s., kteří se podíleli na přípravě této nabídky, tak činili s maximálním úsilím a odbornou znalostí ve snaze maximálně a úplně reagovat na poptávku Vaší společnosti. Věříme, že Vás naše nabídka a návrh v ní obsažený zaujme a budeme pro Vás i nadále kvalitními partnery.

Tato nabídka obsahuje informace, které nejsou určeny ke zveřejnění mimo Vaši organizaci a nesmí být jako celek ani částečně kopírována, upravována ani jinak využívána k účelům, které nesouvisejí s jejím vyhodnocením. Pokud by tato nabídka vedla k uzavření kontraktu, má Vaše organizace právo ji kopírovat či jinak používat při realizaci předmětného kontraktu. Tímto není nijak omezeno právo zákazníka nakládat s informacemi obsaženými v této nabídce, pokud byly získány z jiného zdroje.

Děkujeme Vám za čas, který jste věnovali prostudování naší nabídky. V případě doplňujících dotazů se na nás můžete kdykoliv obrátit. Po vzájemné dohodě jsme připraveni Vás znovu navštívit, poskytnout Vám další informace a pokračovat v načatých jednáních, které doufáme, povedou k Vaší plné spokojenosti. Doufáme, že naše nabídka splní Vaše očekávání a bude se tak moci stát základním kamenem našeho budoucího partnerství na poli informační bezpečnosti.

Za společnost Aricoma Enterprise Cybersecurity a.s.

[redacted]

Katarína Kačengová

Business Security Consultant

Aricoma Enterprise Cybersecurity a.s.

7. Příloha A – Reference

Nedílnou součástí nabídky je samostatný dokument s referencemi.

8. Příloha B – Realizační tým

Nedílnou součástí nabídky je samostatný dokument s popisem realizačního týmu.