ALEF

Trust the Strong

Předmět nabídky:

Penetrační testy pro Akademii múzických umění v Praze

OBSAH

1 Úvod

1.1 Účel dokumentu

Tento dokument obsahuje nabídku na penetrační testy pro Akademii múzických umění v Praze.

1.2 Zákazník

Název společnosti:	**Akademie múzických umění v Praze (dále Zákazník)**
Sídlo:	Malostranské náměstí 259/12, 118 00 Praha 1
IČ:	61384984

1.3 Dodavatel

Název společnosti:	**ALEF NULA, a.s. (dále Dodavatel)** společnost je zapsaná v obchodním rejstříku Městského soudu v Praze, oddíl B., vložka 2727
Sídlo:	Pernerova 691/42, 186 00 Praha 8
IČ:	61858579
DIČ:	CZ61858579
Bankovní spojení:	Komerční banka, a.s.
č. účtu:	51-3717150237/0100
Jednající:	Milan Zinek, předseda představenstva
Telefon:	+420 225 090 111

1.4 Zástupce Dodavatele

Zástupcem dodavatele pověřený jednáním v souvislosti s touto obchodní nabídkou je Daniel Neumann, daniel.neumann@alef.com, +420 702 235 680.

1.5 Platnost nabídky

Tato nabídka je platná do 31.1.2024

2 Informace o Dodavateli

2.1 Profil společnosti

Společnost ALEF NULA a.s. je předním dodavatelem zákaznických řešení pro aplikační a komunikační infrastrukturu v České republice a je součástí nadnárodní skupiny Alef Group, působící v několika zemích střední a východní Evropy.
Nejvyšší prioritou společnosti je dlouhodobá spokojenost zákazníků – tedy pozorné vnímání jejich potřeb a realizace řešení v nejvyšší kvalitě. I proto se ALEF NULA a.s. už od svého založení v roce 1994 orientuje na produkty renomovaných výrobců.
Kvalita služeb ALEF NULA a.s. je opřena o špičkové know-how, rozsáhlé zkušenosti i odborné certifikace v řadě dalších oblastí – od infrastruktury po aplikace, včetně řízení kybernetické bezpečnosti a řízení enterprise a solution architektury. ALEF NULA a.s. svým zákazníků poskytuje konzultační služby, rychlou servisní podporu a školení. ALEF NULA a.s. patří mezi největší školicí střediska v Evropě.
Systém řízení jakosti ALEF NULA a.s. je ve shodě:
s normou ISO 9001:2008.
s normou ISO 27001:2013

ALEF NULA je držitelem oprávnění pro manipulaci s informacemi v úrovni T (tajné) podle zákona Sb. 412/2005
CSIRT ALEF je certified týmem pro oblast Security Operation podle organizace Trusted Introducer.

Aktuálně se kybernetické bezpečnosti ve společnosti intenzivně věnuje více než třicet specialistů, konzultantů a architektů.

Naši zaměstnanci disponují uznávanými certifikáty z různých oblastí kybernetické bezpečnosti, z nichž některé jsou unikátní v rámci České republiky. Za zmínku stojí zejména mezinárodní certifikáty asociace CompTIA (CySA+, PenTest+, CASP, Pentest+), certifikáty v oblasti řízení ISMS (CISM, CISSP, CRISC), certifikáty podporující znalosti penetračního testování (CEH, OPST, ECSA, eJPT, GWAPT) a certifikace v oblasti zvládání incidentů (CCNA Cyber Ops, OPSA, CFR, SIM3). Alef Nula je také držitelem certifikátu Trusted introducer v úrovni „certified“. Teoretické znalosti jsou samozřejmě podporovány dlouholetou zkušeností z úspěšných projektů v oblasti řešení kybernetické bezpečnosti jak u komerčních subjektů, tak i veřejných zadavatelů.

Bezpečnostní služby Alef Nula zahrnují širokou škálu oblastí od zavádění/řízení/přezkoumání ISMS, přes aktivity spojené s návrhem bezpečnostní strategie/politik/procesů až po práce zahrnující návrh designu a provoz SOC/CSIRT. Za zmínku také stojí nabídka služeb spojená s přípravou a realizací security awareness programu, který stavíme na míru zákazníkům ve spolupráci s naším trainingovým centrem. Dále se zaměřujeme na činnosti v oblastech network, aplication a endpoint security, kde naše služby podporují

produkty výrobců CISCO, F5, NetApp, Splunk, Flowmon a dalších. Dílčí aktivity pak směřujeme do oblastí jako jsou NAC, PAM, vícefaktorová autentizace, PKI a windows security.

2.2 Produktové certifikace ALEF NULA a.s.

Níže jsou uvedeny vybrané certifikace společnosti ALEF NULA, a.s.

- Cisco Gold Certified Partner,
- Cisco Advanced Collaboration Architecture Specialized Partner,
- Cisco Advanced Data Center Architecture Specialized Partner,
- Cisco Advanced Enterprise Networks Architecture Specialized Partner,
- Cisco Advanced Security Architecture Specialized Partner,
- Cisco Advanced Service Provider Architecture Specialized Partner,
- Cisco Express Specialized Partner,
- Cisco Learning Partner,
- Cisco Solution Partner.
- 2Ring Partner,
- AWS Consulting Partner,
- AWS Solution Provider & Training Partner,
- ATECO Partner,
- Commvault Partner,
- F5 Authorized Training Center,
- Flowmon Gold Partner,
- Microsoft Gold Technology Partner,
- MobileIron Partner,
- NetApp Contract Delivery Partner,
- Sewio Certified Partner,
- SPLUNK Associate Partner,
- VMware Solution Provider – Enterprise Partner,
- ZOOM Gold Partner.

3 Popis projektu

3.1 Penetrační testy

Předmětem dodávky je realizace jednorázového penetračního testu systémů SDG – single digital gateway a KOS – studijního systému (dle zvolené varianty). Cílem testování je odhalení případných zranitelností a konfiguračních nedostatků ve zmíněných systémech, které by potenciální útočník mohl zneužít k útokům na organizaci nebo uživatele aplikace, za účelem jejich následného odstranění a zvýšení bezpečnosti.

Při realizaci bezpečnostních testů není možné garantovat absenci dopadů na dostupnost testovaných systémů. V případě zjištění omezené dostupnosti cílového systému nebo určité služby v důsledku testů, uvědomí testovací tým o situaci neprodleně kontaktní osobu na straně Zákazníka.

Penetrační testy budou realizovány v předem dohodnutém termínu. Testy mohou začít po poskytnutí všech informací a přístupů požadovaných testovacím týmem a budou provedeny z veřejných IP adres Dodavatele (193.239.0.0/22).

Jednotlivé části popsané níže lze objednat i samostatně.

3.2 Penetrační test SDG – single digital gateway – varianta 1

Objednatel požaduje penetrační test webové aplikace SDG – single digital gateway (https://www.amu.cz/cs/digibrana/). SDG je přihlašovací brána a plní funkci centrálního bodu pro autentizaci uživatelů za účelem podávání a správy přihlášek a s tím spojené financování (platba za přihlášku atd.). Systém jako celek se tedy skládá ze dvou komponent:

- Žádost o financování (https://prihlaska.amu.cz/apps/kos/prihlaska/wpr_stip_pg.main)
- Přihláška ke studiu (https://prihlaska.amu.cz/apps/kos/prihlaska/)

Služby běží na dvou URL adresách.

Penetrační test bude zaměřen především ale nejen na funkcionality vlastní autentizace a autorizace uživatele. Testování bude probíhat v testovacím prostředí a bude zaměřeno na obcházení autentizace/autorizace, neoprávněný přístup k údajům o účtu, neoprávněnou manipulaci s existující identitou, session leaking, autorizaci jednotlivých akcí podmíněných přihlášením, neoprávněnou manipulaci s cizí přihláškou, únik osobních dat a další kritické scénáře.

Testování bude provedeno formou full-knowledge (white-box) testu. Testovací tým bude mít od zákazníka k dispozici veškeré potřebné informace (včetně zdrojového kódu aplikace) s možností se doptat na detaily.

Testování bude probíhat výhradně v testovacím prostředí a testovacímu týmu budou pro test poskytnuty dedikované účty. Vybrané funkcionality (jako je například platba za přihlášku) mohou být po dohodě se zákazníkem testovány v produkčním prostředí nebo budou simulovány v testovacím prostředí. Testování bude probíhat podle aplikovatelných a relevantních kapitol současné verze metodiky OWASP Web Security Testing Guide (OWASP WSTG) a bude se zaměřovat především na zranitelnosti popsané v rámci dokumentu OWASP Web Top 10.

3.3 Penetrační test SDG – single digital gateway + code review – varianta 2

Tato varianta obsahuje vše, co varianta 1 a bude doplněna o automatizovanou statickou analýzu kódu aplikace (SAST) a manuální code review. Přihlašovací brány bezpečnostním specialistou. Testovacímu týmu bude dodán zdrojový kód (PHP cca 200 řádků a PL/SQL cca 17000 řádků) aplikace a bude provedena jeho analýza za účelem identifikací zranitelností, chyb v syntaxi, chyb v rozhodovacích pravidlech a dalších špatných programátorských praktik (složitost kódu, udržovatelnost, testovatelnost …).

Tento typ testů může odhalit další zranitelnosti jako jsou buffer overflow, specifické SQL injection, neošetřené výjimky a další problémy, které by mohly vést například k nestabilitě aplikace.

Dle best practice je rychlost manuální inspekce kódu stanovena na maximálně 500 LOC (lines of code) za hodinu.

3.4 Penetrační test KOS – studijní systém

Předmětem dodávky je realizace jednorázového penetračního testu KOS informačního studijního systému. Testování se bude zaměřovat na webovou aplikaci, do které přistupují zaměstnanci, i studenti. Penetrační testy budou realizovány formou partial-knowledge (grey box) testu a testovací tým bude testovat aplikaci z pohledu jak neautentizovaného uživatele, tak z pohledu uživatele autentizovaného, kdy budou Zákazníkem poskytnuty dva testovací účty s právy studenta a dva testovací účty s právy učitele. Aplikace jako taková je napsána v programovacím jazyce JAVA a skládá se přibližně z 55 stránek, z toho přibližně 16 kritických stránek, kam uživatel může zadávat data, bude definováno Zákazníkem pro detailnější otestování.

Cílem testů bude především ověřit, zda případný útočník nemůže přistupovat k datům, ke kterým nemá přístup, provádět neoprávněné akce, ohrozit integritu dat nebo dostupnost systému.

Penetrační testování webové aplikace se zaměří na příslušné zranitelnosti popsané v dokumentu OWASP Top 10 a bude probíhat podle aplikovatelných a relevantních kapitol současné verze metodiky OWASP Web Security Testing Guide.

3.5 Podpora při zátěžových testech

Zákazník projevil zájem o zátěžové testy výše zmíněných aplikací. Vzhledem k povaze takových testů není vhodné takový útok provádět přes veřejnou internetovou síť. Vhodnější je takové testy provádět například z interní sítě.

Dodavatel v rámci této části poskytne podporu a při provedení těchto testů (jako je pomoc při přípravě nástrojů a prostředí, měření odezvy systému a tak dále). Z dat získaných během testů bude vypracována Závěrečná zpráva.

Zákazníkem budou definovány vybrané části aplikace pro test snesitelné zátěže.

3.6 Používané Metodiky

Pro testování budou využity metodiky používané firmou Alef Nula a.s., které vychází z mnohaletých zkušeností jejích bezpečnostních specialistů a kombinují různé frameworky, standardy a best practice postupy. Tyto jsou používány a aplikovány dle konkrétních nároků bezpečnostního testu a řadí se mezi ně mimo jiné:

- Penetration Testing Execution Standard (PTES),
- Open Source Security Testing Methodology Manual (OSSTMM),
- NIST Special Publication (SP) 800-115,
- Metodiky Licensed Penetration Tester (LPT),
- Information Systems Security Assesment Framework (ISSAF),
- Metodiky a standardy organizace Open Web Application Security Project (OWASP):
    - Web Security Testing Guide (WSTG),
    - Mobile Security Testing Guide (MSTG),
    - Application Security Verification Standard (ASVS),
    - OWASP Top 10.
- Pro potřeby evaluace charakteristiky a závažnosti zranitelnosti:

Testovací tým Alef Nula a.s. využívá pro hledání a testování na přítomnost zranitelností jak manuální postupy zmíněné v předchozích metodikách, tak pomocné a automatické nástroje pro specifické prostředí, účel, či služby. Jako příklad lze uvést aplikaci BurpSuite Pro, Tenable Nessus Professional, NMAP, SQLMap, Gobuster, Metasploit Framework a jiné.

3.7 Výstupy z bezpečnostního testování

Výsledky testů budou shrnuty v Závěrečné zprávě. Ta bude obsahovat seznam zranitelností identifikovaných v rámci penetračních testů, jejich detailní popis a ohodnocení jejich závažnosti dle CVSS v4.0 a také doporučení pro jejich odstranění. Přílohy Závěrečné zprávy pak mohou obsahovat výstupy nástrojů či jiné průkazné informace, které by svojí velikostí nebyly vhodné pro formát Závěrečné zprávy.

3.8 Vymezení rozsahu projektu

Mimo zaměření výše popsaného penetračního testování je jakákoli další infrastruktura, virtualizační platformy, aplikace i SW vybavení jiných systémů. Součástí projektu rovněž nebude testování odolnosti jakýchkoli systémů vůči volumetrickým útokům typu DoS (DDoS), testování fyzické bezpečnosti infrastruktury, ani testy užívající phishing nebo jiné sociotechnické postupy. Mimo rozsah projektu je také tvorba jakékoli jiné dokumentace než výše uvedené Závěrečné zprávy.

3.9 Požadovaná součinnost k projektu

- Dodání informací potřebných pro jednotlivé vybrané části testování (URL adresy, účty, dokumentace, zdrojový kód …).
- Přidání výjimek v bezpečnostních mechanismech, které by mohly ovlivnit průběh testování pro IP adresní rozsahy dodavatele (193.239.0.0/22).
- Dohoda o termínu, ve kterém bude testování prováděno.
- Zřízení vzdáleného přístupu do testovacího prostředí (pokud je potřeba)
- Určení případných omezení pro testování (časové omezení, omezení pro testování jednotlivých systémů apod.).
- Předání informací o primární kontaktní osobě na straně Zákazníka (jméno, e-mail, telefonní číslo) a zajištění její kontinuální dostupnosti v průběhu testů pro řešení případných neočekávaných situací.
- Předání informací o eskalačním kontaktu na straně Zákazníka (jméno, e-mail, telefonní číslo) a zajištění jeho kontinuální dostupnosti v průběhu testů pro řešení případných neočekávaných situací.

3.10 Termín realizace

Přepokládaný termín realizace je duben 2024 či později.

4 Reference bezpečnostních projektů

4.1 Implementace bezpečnostních systémů

Vybrané implementace v oblasti řízení informační bezpečnosti ICT:

- Generální ředitelství cel
- Český hydrometeorologický ústav
- Krajský úřad Jihočeského kraje
- ČEZ Distribuce, a.s.
- Mero ČR a.s.
- NET4GAS, s.r.o.
- Krajská Nemocnice Liberec, a.s.
- Ad. …

4.2 Bezpečnostní služby a poradenství

Vybrané služby v oblasti bezpečnostního auditu, bezpečnostního designu a poradenství:

- Český hydrometeorologický ústav
- Komerční banka, a.s.
- ERA a.s.
- Energetický regulační úřad
- Moravskoslezský kraj
- Institut klinické a experimentální medicíny
- Krajský úřad Olomouckého kraje
- Krajský úřad Pardubického kraje
- Krajský úřad Ústeckého kraje
- Ministerstvo průmyslu a obchodu
- České dráhy
- Generální ředitelství cel
- Zdravotnická záchranná služba Jihomoravského kraje
- Ad. …

5 Cenová nabídka

Penetrační test SDG – single gateway – varianta 1

Název položky	Cena v Kč bez DPH
Penetrační test	
Vytvoření Závěrečné zprávy	
Celková cena	**90 000 Kč bez DPH**

Penetrační test SDG – single digital gateway + code review – varianta 2

Název položky	Cena v Kč bez DPH
Penetrační test	
SAST analýza cca 17200 řádků kódu	
Vytvoření Závěrečné zprávy	
Celková cena	**288 000 Kč bez DPH**

Penetrační test KOS – studijní systém

Název položky	Cena v Kč bez DPH
Penetrační test	
Vytvoření Závěrečné zprávy	
Celková cena	**210 000 Kč bez DPH**

Podpora při zátěžových testech

Název položky	Cena v Kč bez DPH
Příprava podkladů	
Asistence při provádění	
Závěrečná Zpráva	
Celková cena	**36 000 Kč bez DPH**

5.1 Platební podmínky

Splatnost faktur je 30 dní.