

Bezpečnostní analýza Microsoft 365 - nabídka



Obsah

1. Úvod	3
1.1. Účel dokumentu	3
1.2. Dodavatel.....	3
1.3. Zástupce Dodavatele	3
1.4. Platnost nabídky.....	3
2. Informace o Dodavateli	4
2.1. Profil společnosti	4
2.2. Produktové certifikace ALEF NULA a.s.	5
3. Shrnutí požadavků Zákazníka	6
4. Popis navrženého řešení	6
4.1. Vymezení rozsahu projektu	6
5. Reference bezpečnostních projektů	9
5.1. Implementace bezpečnostních systémů.....	9
5.2. Bezpečnostní služby a poradenství	9
6. Cenová nabídka	10
6.1. Rozpis ceny.....	10
6.2. Platební podmínky.....	10

1. Úvod

1.1. Účel dokumentu

Tento dokument obsahuje nabídku na bezpečnostní analýzu prostředí Microsoft 365.

Název společnosti: **Akademie múzických umění v Praze**

Sídlo: Malostranské náměstí 259/12, 118 00 Praha 1

IČ: 61384984

1.2. Dodavatel

Název společnosti: **ALEF NULA, a.s. (dále Dodavatel)**

společnost je zapsaná v obchodním rejstříku Městského soudu v Praze, oddíl B., vložka 2727

Sídlo: Perneroва 691/42, 186 00 Praha 8

IČ: 61858579

DIČ: CZ61858579

Bankovní spojení: Komerční banka, a.s.

č. účtu: 51-3717150237/0100

Jednající: Milan Zínek, předseda představenstva

Telefon: +420 225 090 111

Fax: +420 225 090 112

1.3. Zástupce Dodavatele

Zástupcem dodavatele pověřený jednáním v souvislosti s touto obchodní nabídkou je Jan Hembera, jan.hembera@alef.com, tel.: +420 731 635 050.

1.4. Platnost nabídky

Tato nabídka je platná po dobu 30 dnů od vystavení nabídky.

2. Informace o Dodavateli

2.1. Profil společnosti

Společnost ALEF NULA a.s. je předním dodavatelem zákaznických řešení pro komunikační infrastrukturu v České republice a je součástí nadnárodní skupiny Alef Group, působící v několika zemích střední 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, především společnosti Cisco Systems. V této souvislosti je ALEF NULA a.s. držitelem nejvyšší partnerské certifikace Cisco Systems Partner – Gold Certified.

Kromě implementačních projektů tradiční LAN/WAN infrastruktury má ALEF NULA a.s. špičkové know-how, rozsáhlé zkušenosti i odborné certifikace v řadě dalších produktových oblastí – od datových center, přes síťovou bezpečnost a wireless až po IP telefonii, videokonferenční řešení a kontaktní centra. K tomu poskytuje ALEF NULA svým zákazníkům i konzultační služby, rychlou servisní podporu a školení. ALEF NULA je držitelem certifikace Cisco Learning Partner a patří mezi pět největších školicích středisek technologie Cisco v Evropě.

System řízení jakosti ALEF NULA a.s. je ve shodě s normou ISO 9001:2008.

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,
- Veeam Silver Partner.

3. Shrnutí požadavků Zákazníka

Zákazník pro své potřeby používá služeb Microsoft 365 a v rámci zvyšování úrovně zabezpečení svého prostředí poptává bezpečnostní analýzu svého prostředí. Zákazník aktivně používá služby Microsoft Entra ID, Microsoft Entra Connect, Exchange Online, SharePoint a OneDrive a Defender for Office 365. Provedeme bezpečnostní analýzu těchto služeb pro identifikaci možných zranitelností plynoucích z konfigurace a vlastností stávajícího prostředí. Výstupní dokumentace bude obsahovat doporučení pro jejich minimalizaci v souladu s vyhláškou o kybernetické bezpečnosti.

4. Popis navrženého řešení

Bezpečnostní analýzu provádíme na základě doporučení společnosti Microsoft, Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB), zkušeností z praxe, Center for Internet Security (CIS), National Institute of Standards and Technology (NIST) a dalších doporučení bezpečnostních organizací, ze kterých jsme sestavili sadu otázek týkající se konfigurace jednotlivých úseků prostředí Microsoft 365 a také s nimi spojených procesů. Jednotlivé úseky se skládají z následujících bodů.

4.1. Vymezení rozsahu projektu

Cílem projektu je poskytnout zákazníkovi komplexní analýzu zabezpečení prostředí Microsoft 365 a to v posloupnosti naznačené níže.

4.1.1. Microsoft Entra ID (dříve Azure Active Directory)

Microsoft Entra ID je kritický systém pro chod cloudového prostředí Azure a Microsoft 365. Uchovávají se zde informace o všech synchronizovaných a cloudových objektech společnosti (identity, skupiny, zařízení atd.), proto je třeba zabezpečit přístup do tohoto prostředí, a to nejen administrátorům, ale i běžným uživatelům.

Cílem analýzy je:

- 1) Prověření stávající konfigurace (nastavení spolupráce s externisty, skupiny, podmíněný přístup, logování, retence logů, privileged identity management atd.)
- 2) Dokumentace s případným doporučením ke změně

Součástí analýzy není:

- 1) Změny v konfiguraci

Požadovaná součinnost zákazníka:

- 1) Přístup globálního správce v režimu čtení / součinnost se správcem prostředí
- 2) Vyhrazený čas správce prostředí pro diskusi ohledně procesních záležitostí

4.1.2. Microsoft Entra Connect (dříve Azure AD Connect)

Microsoft Entra Connect je synchronizační nástroj společnosti Microsoft, který tvoří most mezi on-premise prostředím a cloudem. Nesprávná konfigurace tohoto nástroje může jednoduše vyústit v bezpečnostní rizika, která mohou ovlivnit celý chod společnosti.

Cílem analýzy je:

- 1) Prověření stávající konfigurace, zabezpečení a instalace
- 2) Dokumentace s případným doporučením ke změně

Součástí analýzy není:

- 1) Konfigurace synchronizačního nástroje

Požadovaná součinnost zákazníka:

- 1) Poskytnutí informací o synchronizačním nástroji
- 2) Poskytnutí informací o serveru, na kterém je aplikace nainstalovaná

4.1.3. Exchange Online + Exchange Online Protection (EOP)

Exchange Online je služba pro interní i externí komunikace. Jde o významný informační systém zákazníka umístěný v prostředí Microsoft 365. Nastavení zmíněného systému musí odpovídat vyhlášce o kybernetické bezpečnosti.

Cílem analýzy je:

- 1) Prověření stávající konfigurace (nastavení spam filtrů, malware filtrů, karantén, DKIM, DMARC, SPF atd.)
- 2) Dokumentace s případným doporučením ke změně

Součástí analýzy není:

- 1) Změny v konfiguraci

Požadovaná součinnost zákazníka:

- 1) Přístup globálního správce v režimu čtení / součinnost se správcem prostředí
- 2) Vyhrazený čas správce prostředí pro diskusi ohledně procesních záležitostí

4.1.4. SharePoint Online & OneDrive

Veškerá firemní aktiva končí převážně na službách SharePoint Online a OneDrive. Vzhledem k tomu, jak jednoduše jednotlivé weby mohou vznikat, budeme se zajímat o aktivní weby služby SharePoint

Online & OneDrive a jejich zásady pro sdílení dat a následně jak nové weby služby SharePoint Online mohou vznikat.

Cílem analýzy je:

- 1) Prověření stávající konfigurace (nastavení celo-organizačních zásad služeb, nastavení zásad na jednotlivých webech, způsob řízení oprávnění atd.)
- 2) Dokumentace s případným doporučením ke změně

Součástí analýzy není:

- 1) Změny v konfiguraci

Požadovaná součinnost zákazníka:

- 1) Přístup globálního správce v režimu čtení / součinnost se správcem prostředí
- 2) Vyhrazený čas správce prostředí pro diskusi ohledně procesních záležitostí (vytváření nových webů, řízení oprávnění nad jednotlivými weby atd.)

4.1.5. Analýza Defender for Office 365

Součástí Defender for Office 365 je řada nástrojů sloužících ke komplexní ochraně prostředí Microsoft 365. V prostředí zákazníka je však pouze ojedinělý počet licencí Microsoft 365 E5, a tudíž většina funkcionalit v Defender for Office 365 není aplikována na majoritu uživatelů. Součástí analýzy jsou pouze okruhy, které spadají do licenčních balíčků, které jsou dostupné majoritě uživatelů zákazníka.

Cílem analýzy je:

- 1) Prověření konfigurace Anti-malware, Anti-phishing, Anti-spam
- 2) Prověření konfigurace Safe Links, Safe Attachments, Zero-hour Auto Purge

Součástí analýzy není:

- 1) Změny v konfiguraci
- 2) Analýza sekce Cloud Apps
- 3) Analýza sekce Assets
- 4) Analýza sekce Incidents and alerts
- 5) Analýza sekce Hunting
- 6) Analýza sekce Threat intelligence

Požadovaná součinnost zákazníka:

- 1) Přístup globálního správce v režimu čtení / součinnost se správcem prostředí
- 2) Vyhrazený čas správce prostředí pro diskusi

5. Reference bezpečnostních projektů

5.1. 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. ...

5.2. 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. ...

6. Cenová nabídka

Cenová nabídka je rozdělená na části podle přechozích bodů, a to v posloupnosti, ve které doporučujeme danou analýzu provést. Předmětem nabídky je realizace této analýzy a tvorba dokumentace zachycující aktuální stav prostředí Microsoft 365 a doporučení nápravných opatření.

6.1. Rozpis ceny

Celková cena za předmět nabídky je 235 000,00 Kč bez DPH.

Vypracoval:	Martin Strnad	Datum:	12.02.2024
Telefon:	734754544	Klasifikace:	Důvěrné
Email:	martin.strnad@alef.com		
Název projektu	Popis služby	Cena celkem	
Bezpečnostní analýza identitního systému		105,000 CZK	
	Analýza Microsoft Entra ID		
	Analýza Microsoft Entra Connect		
	Příprava výstupní dokumentace		
	Shrnutí nalezených zranitelností a nápravných opatření		
	Administrativa a řízení projektu		
Bezpečnostní analýza systému elektronické pošty		80,000 CZK	
	Analýza Exchange Online + Exchange Online Protection (EOP)		
	Analýza Defender for Office 365		
	Příprava výstupní dokumentace		
	Shrnutí nalezených zranitelností a nápravných opatření		
	Administrativa a řízení projektu		
Bezpečnostní analýza ostatních služeb		50,000 CZK	
	Analýza SharePoint Online & OneDrive		
	Příprava výstupní dokumentace		
	Shrnutí nalezených zranitelností a nápravných opatření		
	Administrativa a řízení projektu		
		235,000 CZK	

6.2. Platební podmínky

Splatnost faktur je 30 dní.