Příloha č. 2

**TECHNICKÁ SPECIFIKACE**

|  |  |
| --- | --- |
| **Název veřejné zakázky** | **„**Služby IT **SOŠ a SOU, Vocelova 1338“** |

Technická specifikace zahrnuje specifikaci HW a SW vybavení, včetně požadované správy, konfigurace a aktualizace jednotlivých prvků. Dále specifikace zahrnuje monitorování celé IT infrastruktury, které bude zajišťováno pomocí automatizace a powershellových scriptů, a také specifikaci bezpečnostních opatření pro minimalizaci rizik v oblasti bezpečnosti IT prostředí.

**1. Servery:**

1.1 Správa serverového HW a aktualizace firmwaru pro 1 HW server (Dell) a 4 virtuální servery

1.2 Monitoring zdraví a výkonu serverů

**2. Virtualizace serverů:**

2.1 Použitá technologie Hyper-V

**3. Router:**

3.1 Správa bezpečnostního firewallu a segmentace sítě

3.2 Analýza síťového provozu

Poskytovatel bude zodpovědný za správu a údržbu všech routerů, včetně segmentace sítě a aktualizace firmware. Bude muset mít znalost topologie sítě a bude schopen identifikovat problémy s konfigurací sítě a případně je vyřešit.

- Použitá technologie Fortinet Fortigate

**4. Switche:**

4.1 Správa sítě a segmentace

4.2 Upgrade firmware a znalost topologie

4.3 Celkem 25 kusů

Poskytovatel bude zodpovědný za správu a údržbu všech 25 switchů, včetně segmentace sítě a aktualizace firmware. Bude muset mít znalost topologie sítě a bude schopen identifikovat problémy s konfigurací sítě a případně je vyřešit.

- Použitá technologie Unifi

**5. Wifi:**

5.1 Centrální správa

5.2 Upgrade firmware

5.3 Cca. až 500 připojených zařízení

5.4 Celkem 30 kusů

Poskytovatel bude zodpovědný za centrální správu 30 wifi zařízení a upgrade firmware. Celkově bude muset zvládat až 500 připojených zařízení a bude muset být schopen identifikovat problémy s připojením a vyřešit je.

- Použitá technologie Unifi

**6. Antivirové řešení:**

6.1 Denní vyhodnocování výstupů AV a jejich odborná interpretace

6.2 Centrální správa

Poskytovatel bude zodpovědný za denní vyhodnocování výstupů antivirového řešení a bude muset mít odborné znalosti pro interpretaci výsledků. Také bude zodpovědný za centrální správu řešení a bude muset být schopen identifikovat a odstranit hrozby a infekce.

- Použitý antivir ESET NOD32

**7. Síťové logy:**

7.1 Denní vyhodnocování a archivace síťové komunikace a jejich odborná interpretace

Poskytovatel bude zodpovědný za denní vyhodnocování síťových logů a archivaci komunikace. Bude muset mít odborné znalosti pro interpretaci výsledků a bude zodpovědný za identifikaci a odstranění případných bezpečnostních hrozeb.

- Použitá technologie Fortinet FortiAnalyzer

**8. Monitoring celého prostředí:**

8.1 Monitoring serverů, stanic, sítě a IOT zařízení

8.2 Zpětná vazba zajišťující pečlivost celé správy pomocí automatizace a powershellových scriptů

8.3 Patchmanagement

Poskytovatel bude zodpovědný za monitorování celého prostředí, včetně serverů, stanic, sítě a IOT zařízení. Bude muset mít odborné znalosti pro správu a údržbu těchto prvků a bude schopen identifikovat a odstranit případné problémy.

- Použitý program N-ABLE

**9. Password a session manager:**

Poskytovatel poskytne Zadavateli licence a implementaci Devolution serveru pro centralizovanou správu hesel a session manageru. Devolution server umožňuje správu přístupových údajů k různým systémům a aplikacím včetně jejich rotace a auditu přístupů. Zároveň poskytuje možnost sdílení přístupových údajů mezi uživateli s různými oprávněními.

- Použitá technologie Devolution server

**10. Zabezpečený Terminálový Jump server pro bezpečnou správu**

Zabezpečený Terminálový Jump server pro bezpečnou správu: Poskytovatel zajistí implementaci a konfiguraci terminálového serveru, který umožní vzdálenou správu serverů a aplikací s vysokou mírou zabezpečení. Terminálový server umožňuje vzdálenou správu pomocí protokolu SSH a připojení k serverům a aplikacím skrz tzv. "jump host". Poskytovatel zajistí konfiguraci dostatečného zabezpečení terminálového serveru pro minimalizaci rizik spojených s vzdáleným přístupem k citlivým datům a aplikacím ve vlastním datacentru. (vítěz tohoto VŘ).

**11. Ostatní požadavky**

• **Dostupnost:** Poskytovatel bude mít vždy k dispozici dostatečné množství techniků, kteří budou schopni rychle reagovat v případě výpadků nebo poruch. V případě potřeby bude Poskytovatel schopen poskytnout Zadavateli technickou podporu 24 hodin denně, 7 dní v týdnu.

• **Zálohování dat**: Poskytovatel zajistí pravidelné zálohování všech dat, která jsou uložena na serverech školy. Zálohy budou prováděny v určitých časových intervalech a budou ukládány na bezpečném místě mimo školní areál pro jejich obnovení v případě potřeby, a to v současnosti pomocí Veeam Backup & Replication.

**• Aktualizace softwaru a firmware:** Poskytovatel zajistí pravidelnou aktualizaci veškerého softwaru a firmware, který je využíván na serverech a síťových prvcích školy. Aktualizace budou probíhat v koordinaci se Zadavatelem, aby minimalizovaly možné výpadky a nepříjemnosti pro uživatele.

• **Bezpečnost**: Poskytovatel zajistí, že veškerá komunikace mezi zařízeními bude zabezpečena šifrováním, a všechny přístupy k citlivým datům budou chráněny heslem. Poskytovatel bude pravidelně provádět audit bezpečnostních opatření, aby zajistil, že jsou všechny prvky sítě školy řádně chráněny před hrozbami.

**• Zpracování osobních údajů**: Poskytovatel bude dodržovat všechny platné zákony a předpisy týkající se ochrany osobních údajů. Všechny informace, které budou poskytnuty Poskytovateli v rámci této Smlouvy, budou považovány za důvěrné a budou použity pouze k účelům, pro které byly poskytnuty.

• **Reporting**: Poskytovatel bude pravidelně poskytovat Zadavateli reporty o výkonu sítě a serverů školy, včetně informací o využívání kapacity, zátěži a výpadcích. Tyto reporty pomohou Zadavateli.

• **Správa emailového prostředí** – zajištění bezpečnosti a správy emailového prostředí v současnosti pomocí Microsoft Exchange Server.

• **Správa Active Directory** – správa uživatelských účtů a skupin v prostředí Windows Active Directory,

cca 800 uživatelů.

• **Správa cloudových služeb** – správa a monitorování cloudových služeb, jako je Office 365 a Azure.

**• Konzultace** – Poskytnutí odborné konzultace při řešení problémů v IT prostředí.

**• Vzdálená správa** v současnosti primární TeamViewer, sekundární Take Control, cca *350 stanic*

• **Případná změna** v současnosti provozovaných technologií je zahrnuta v nabídnuté ceně.

**• Školení** - poskytnutí školení pro zaměstnance školy týkající se používání IT zařízení a služeb.

• **20 hodin** vyžádaných prací, mimo výše uvedené služby, konaných dle potřeby buď vzdáleně, nebo v místě plnění (v rámci nabídkové ceny).

**• Zápůjčka HW** v případě selhání.

• **Správa tiskáren** - 10 kusů

• **Správa školního NAS,** v současnosti Synology

**Poznámka:**

Technologie, výrobci a obchodní názvy jsou aktuálně nasazená řešení ve školní síti.