Technická specifikace, část Intune

Úvod

Tento dokument specifikuje požadavky na provedení analýzy stávající IT infrastruktury a na nasazení platformy **Microsoft Intune** jako hlavního nástroje pro správu koncových zařízení v prostředí **Ostravské univerzity**.

Cílem této části projektu **VIVAT OU** je:

- zavést **Microsoft Intune** jako primární systém pro správu zařízení s operačními systémy Windows, Windows Server a Android v rámci sítě OU
- umožnit **hybridní nebo plně cloudovou správu** těchto zařízení
- **nahradit nebo doplnit** dosavadní on-premises nástroje (Active Directory Group Policy a SCCM)
- **integrovat správu Apple zařízení s operačními systémy MacOS, iPadOS a iOS** prostřednictvím napojení na **Apple School Manager (ASM)**, integrovat správu zařízení s operačním systémem **Linux** a integrovat správu zařízení **Google**
- **proškolit správce OU** v oblasti správy platformy Intune

Požadované řešení musí být navrženo v souladu s osvědčenými postupy společnosti **Microsoft** a zároveň musí umožnit integraci se službami **Microsoft Defender for Endpoint** a **Windows Autopilot**.

1. Výchozí stav

V současnosti využíváme on-premises Active Directory se synchronizací Entra Connect do prostředí Microsoft 365. Prostředí OU obsahuje cca 20 000 uživatelů (pokryto licencemi EES A1, A3, A5). Active Directory obsahuje cca 2 000 zařízení (Windows a Windows Server), bez synchronizace do Microsoft 365. Endpoint protection těchto zařízení je spravovaná nástroji rodiny ESET, tyto nástroje budou pravděpodobně nahrazeny nástrojem Microsoft Defender for Endpoint. Na zařízení připojená do Active Directory jsou aplikovány desítky politik GPO. K dispozici máme také nástroj SCCM, který není aktivně využívaný. BYOD zařízení nejsou nijak řešena. Apple School Manager je aktivní a používaný pro registraci všech Apple zařízení v majetku OU. K dispozici máme tenant Google Workspace for Education, který aktivně využívají stovky uživatelů.

2. Předmět poptávané služby (specifikace)

Analýza, návrh architektury a všech dílčích konfigurací musí být rozděleny na implementaci pilotního provozu pro vymezenou testovací skupinu uživatelů a zařízení a pro cílový celo-organizační produkční provoz.

2.1 Analýza a návrh architektury

- **Posouzení aktuálního prostředí** (on-premises AD, Microsoft 365/Entra a návazné portály a platformy jako jsou Security nebo Compliance, GPO, SCCM, bezpečnostní politiky, Apple School Manager), definice technických prerekvizit
- **Analýza licenčních prerekvizit**, případně návrh licenční potřeb
- **Analýza lidských zdrojů,** specifikace nároků na správu navržené architektury oproti stávajícímu stavu
- **Návrh cílové architektury:**
    - Intune-only, nebo Hybrid Join / Co-Management
    - Intune + **Autopilot**
    - Návrh **bezpečného řízení a oprávnění** k Intune a Autopilot
    - Rozhraní mezi Intune a **SCCM** (pokud bude zachován)
    - Rozhraní mezi Intune a **Apple School Manager**
    - Analýza a specifikace možností řízení a monitoringu **BYOD zařízení**
    - Analýza možnosti integrace s **Google Workspace** a **správy ChromeOS** zařízení, posouzení možností synchronizace identit mezi Microsoft 365 a Google Workspace (včetně SAML a SCIM), návrh způsobu správy ChromeOS zařízení prostřednictvím Google Admin Console v Google Workspace for Education
    - Návrh a **doporučení v oblasti centrálního auditu, monitoringu a logování**, používáme nástroje LogManager, Nagios, Zabbix
    - **Návrh způsobu registrace zařízení** (Autopilot, GPO, manuální, MDM enrollment, návrh aplikačních politik)
    - **Návrh segmentace** uživatelů/skupin
    - Návrh vhodných **Compliance policies** s ohledem na bezpečnostní nastavení a bezpečnostní normy a politiku OU
    - Návrh vhodných **Configuration profiles** dle typů spravovaných zařízení
    - Návrh vhodných **Endpoint Security profiles** dle typů spravovaných zařízení

2.2 Implementace a nastavení Intune

- Nastavení **Intune** (natavení MDM authority, nastavení politik atd.)
- Integrace s Entra Conditional Access, návaznost na nastavení MFA a compliance zařízení, integrace s Role-Based Access Control, integrace se zavedenými interními metodickými postupy a nastaveními jako jsou reakce na Entra Risky-Users, či návaznost na metodiku urgentních blokací kompromitovaných uživatelů a zařízení
- Nastavení **Compliance policies**
- Nastavení **Configuration profiles**
- Nastavení **Endpoint Security profiles**
- Integrace se službou Defender for Endpoint (pokud je součástí)
- Nastavení registrace zařízení: Windows 10/11, iOS, iPadOS, MacOS, Linux, Android
- Definice a nastavení škálování správy (různá práva pro správce, fakultní techniky atd.)
- Rozdělení do pilotních skupin, testování
- Nastavení síťových profilů a **802.1X autentizace**, definice a nasazení Wi-Fi a LAN profilů s podporou 802.1X autentizace pro zařízení s Windows, macOS a iOS, ověření kompatibility s existující síťovou infrastrukturou OU
- Případná integrace s NAC ClearPass (pokud bude na OU implementován)

2.3 Autopilot a správa zařízení

- Nastavení **Windows Autopilot** (import zařízení, deployment profily)
- Vytvoření dynamických skupin v Entra pro cílení politik
- Vytvoření aplikačních politik
- Nastavení BitLocker správy (Recovery Keys do Entra ID)

2.4 Migrace stávajících zařízení

- **Strategie migrace:** Zvážení a návrh vhodného způsobu připojení zařízení do Entra (např. přechod z čistě on-premises AD na Hybrid Entra Join nebo přímo Entra Join), včetně posouzení dopadů na správu, bezpečnost a uživatelskou zkušenost a implementace tohoto způsobu včetně migrace stávajících zařízení
- Napojení starších zařízení do Intune (skripty, GPO, PowerShell)
- Správa GPO vs. CSP – převod politik (nástroje jako MDM Migration Analysis Tool)

3. Harmonogram (návrh fází)

V rámci úvodní fáze projektu provede dodavatel detailní analýzu prostředí a identifikuje ve spolupráci se zadavatelem všechny činnosti, které mohou mít vliv na úspěšné nasazení Intune. Výstupem bude plán implementace.

Plán implementace:

- Analýza, konzultace a návrh vhodného harmonogramu implementace
- Pilotní nasazení
- Školení správců, dokumentace
- Rozšíření na produkci a zajištění přechodu na rutinní provoz (v rozsahu, který bude výstupem analýzy a návrhu implementace)

4. Požadované výstupy

4.1 Požadovaný výstup analýzy

Výstupem analýzy a návrhu architektury a jednotlivých konfigurací musí být podrobné a strukturované dokumenty obsahující následující části:

- **Souhrn**, který shrnuje zjištění a doporučení
- Detailní **návrh harmonogramu**, tak aby byla zaručena udržitelnost a bezpečnost provozu
- Návrh **způsobu komunikace** mezi dodavatelem a zadavatelem (formát konzultací, průběh konfigurací, přístupy a oprávnění do prostředí atd.)
- Detailní **popis všech technických a licenčních prerekvizit** nutných k implementaci centrální správy zařízení nástroji Intune a Autopilot
- Detailní **popis každé identifikované jednotlivé konfigurace** či nutné činnosti dle výše zmíněného zadání včetně dopadu na celkové prostředí OU, dopadu na správu prostředí, dopadu na celkové zabezpečení prostředí a dopadu na správce, uživatele a zařízení
- **Návrh přechodu** na nasazení Intune se všemi zmíněnými požadavky v rámci **pilotního nasazení** (pro vymezenou testovací skupinu uživatelů a zařízení)
- **Návrh nasazení** Intune se všemi zmíněnými požadavky **na celou organizaci** (dle výstupu analýzy a konzultací, dle složitosti konfigurací a nároku na správce se může jednat jak o implementaci zadavatelem, tak o předané know-how správcům školeními, metodikou a návody)
- Veškeré dokumenty musí být dodány v obecně rozšířeném formátu vhodném na editaci, práci s textem, kopírování části atd. (např. DOCX, XLSX) a jejich rozsah musí odpovídat komplexitě a rozmanitosti zadání. Dokumenty musí být doplněny o manažerská shrnutí, která zobrazují hlavní body a výstupy zakázky pro vedení a zainteresované strany
- Dokumenty musí být dodány v českém jazyce

4.2 Požadovaný výstup implementace

Po konzultacích mezi dodavatelem a zadavatelem a souhlasu s návrhem architektury a jednotlivých konfigurací ze strany zadavatele musí být dodáno dle výše uvedeného komplexního zadání, a to v souladu s navrženým harmonogramem:

- Funkční **nasazení Microsoft Intune** včetně detailního popisu každé identifikované jednotlivé konfigurace či nutné činnosti dle výše zmíněného zadání včetně dopadu na celkové prostředí OU, dopadu na správu prostředí, dopadu na celkové zabezpečení prostředí a dopadu na správce, uživatele a zařízení
- Funkční **nasazení Windows Autopilot** včetně detailního popisu každé identifikované jednotlivé konfigurace či nutné činnosti dle výše zmíněného zadání včetně dopadu na celkové prostředí OU, dopadu na správu prostředí, dopadu na celkové zabezpečení prostředí a dopadu na správce, uživatele a zařízení
- Úspěšný a bezproblémový provoz **pilotní implementace**
- Nasazení **produkčního provozu** dle výše zmíněné definice
- **Interní školení pro správce** (Intune konzole, Autopilot a další konzole v rámci prostředí Microsoft 365 týkající se správy a nastavení zařízení a jejich zabezpečení, auditu, troubleshootingu atd.)
- Dodání **provozní dokumentace**, tj. popisu konfigurací a postupů včetně možnosti postupného škálování a popisu řešení obvyklých potenciálních problémů jako jsou bezpečnostní postupy v případě kompromitace zařízení, ztráty zařízení, odebrání přístupu kompromitovaného zařízení k firemním datům, odstranění firemních dat z kompromitovaného zařízení, zablokování registrace zařízení nebo jeho odpojení z Microsoft Entra, postupy pro správu zařízení v offline režimu nebo s omezeným připojením atd. Rozsah dokumentace musí odpovídat komplexitě a rozmanitosti zadání
- Dodání návodů pro techniky a uživatele (návody na správu zařízení, manuály na onboarding zařízení)
- Pravidelný souhrn implementace, dle rozsahu domluveného v rámci návrhu způsobu komunikace, který shrnuje aktuální stav, doplněný o manažerské shrnutí, popisující hlavní body a výstupy zakázky pro vedení a zainteresované strany
- Veškeré dokumenty musí být dodány v obecně rozšířeném formátu vhodném na editaci, práci s textem, kopírování části atd. (např. DOCX, XLSX) a jejich rozsah musí odpovídat komplexitě a rozmanitosti zadání.
- Dokumenty musí být dodán v českém jazyce

5. Způsob dodání

Dodavatel je povinen zajistit kompletní a funkční řešení dle účelu projektu, včetně všech návazných činností, které jsou obvyklé a nezbytné pro úspěšné nasazení a provoz platforem Microsoft Intune a Autopilot (včetně všech dílčích požadavků), i pokud nejsou výslovně uvedeny v této specifikaci.

5.1 Řízení a průběh implementace

Konfigurace jednotlivých části pak musí být:

- Aplikace jednotlivých bodů musí být řízena ze strany CIT, veškeré dopady musí být řádně vykomunikovány s vedením projektu a se správci a informace o změnách a dopadech musí být vhodným způsobem předány koncovým uživatelům
- Aplikace jednotlivých bodů může probíhat formou workshopů pro správce i samostatnou konfigurací dodavatelem, dle rozsahu činnosti, složitostí a možností správců CIT, a to vždy na základě domluvy s vedením projektu a správci CIT

6. Závěry

Implementace Intune musí probíhat transparentně, s pravidelným reportováním stavu, a s ohledem na to, že některé komponenty systému jsou (dle vyhlášky č. 317/2014 Sb.) významným informačním systémem a že podle nové legislativy o kybernetické bezpečnosti budou součástí regulované služby univerzity.