Technická specifikace, část MFA

Úvod

Tento dokument specifikuje požadavky na analýzu, přípravu a samotnou implementaci multifaktorové autentizace (MFA) v rámci projektu VIVAT OU.

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

- analyzovat, navázat na stávající technická řešení a navrhnout metodické řízení a **zavést MFA pro všechny identity** v prostředí Ostravské univerzity, to zahrnuje správce systémů, zaměstnance, studenty, externí identity a hosty, v prostředí **Microsoft 365/Entra a návazných platforem**
- analyzovat, navrhnout technická řešení, navrhnout metodické řízení, vytvořit vztah pro synchronizaci identit s identitami OU, implementovat jednotné přihlášení včetně MFA mezi stávajícími systémy a platformou **Google Workspace**
- analyzovat, navrhnout technická řešení, navrhnout metodické řízení a rozšířit stávající autentizační mechanismus **Shibboleth** o multifaktorovou autentizaci
- zohlednit současné metody MFA, zajistit přípravy na implementaci výše zmíněného a implementovat výše zmíněné jako celek

Požadované řešení musí být navrženo v souladu s osvědčenými postupy společnosti **Microsoft**.

1. Výchozí stav

V současné době je multifaktorová autentizace (MFA) povinná pro všechny správce prostředí Microsoft 365/Entra/Azure, uživatele platformy Azure Dev Tools for Teaching (vyučující a studenti), správce Google Workspace, správce proprietárního řešení identity managementu IDM a pro vybrané uživatele Microsoft 365. Mimo rámec tohoto projektu je řešena implementace přechodu z legacy per-user MFA na Authentication Methods Policy. Přechod z legacy per-user MFA na moderní správu autentizačních metod pomocí Authentication Methods Policy je řešen v rámci samostatného předřazeného projektu. V době implementace projektu VIVAT OU bude organizace na tuto změnu připravena a dodavatel na ni může navázat.

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

- **Analýza aktuálního prostředí** (on-premises AD, Microsoft 365/Entra a návazné portály a platformy jako jsou Security nebo Compliance, Google Workspace, Shibboleth) obsahující doporučení adekvátních metod, jejich škálování a doporučení s ohledem na jednotlivé skupiny uživatelů, včetně návrhu a řízení integrace jednotlivých požadovaných komponent
- **Analýza licenčních prerekvizit**, případně návrh licenční potřeb
- **Analýza lidských zdrojů**, specifikace nároků na správu navržené architektury oproti stávajícímu stavu (zavedením MFA na všechny uživatele řádově vzroste nárok na správu a uživatelskou podporu ze strany správců a techniků)
- **Návrh cílové architektury:**
    - Návrh implementace **MFA v prostředí Microsoft 365/Entra** a návazných platforem, včetně návrhu na rozšíření MFA do on-premises Active Directory
    - Návrh implementace **MFA v prostředí Google Workspace**, včetně synchronizace identit a jednotného přihlášení
    - Návrh **rozšíření** autentizačního mechanismu **Shibboleth** o multifaktorovou autentizaci
    - Návrh způsobu registrace uživatelů do MFA systému – **onboarding** (automatizované, manuální, způsoby metod podporovaných faktorů dle příslušnosti ke skupinám, řešení při ztrátě přístupů, či používaného faktoru)
    - Návrh a **doporučení v oblasti centrálního auditu, monitoringu a logování**, používáme nástroje LogManager, Nagios, Zabbix
    - Návrh vhodných **Compliance, Security a Conditional politik** s ohledem na bezpečnostní nastavení a bezpečnostní normy a politiku OU
    - Návrh **metodických postupů a nastavení** návazných na metodiku urgentních blokací kompromitovaných uživatelů a zařízení (jako např. reakce na Entra Risky-Users)

2.2 Implementace a nastavení MFA

- **Kontrola nastavení, rozšíření MFA pro všechny uživatele**, včetně vhodného škálování dle cílových skupin (zaměstnanci, studenti, externí identity, hosté, správci zmíněných technologií atd.)
- Implementace metodiky **on-boardigu uživatelů**
- Integrace s **Entra Conditional Access, Intune** a dalšími bezpečnostními prvky Microsoft 365/Entra, doporučení a konfigurace vhodných nastavení na základě stavu zařízení, geografického určení a sítí
- 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
- Integrace s **Google Workspace**
- **Integrace s** autentizačním mechanismem **Shibboleth**
- Nastavení **Compliance, Security a Conditional politik**
- Rozdělení do pilotních skupin, testování

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 MFA na celou organizaci. Výstupem bude plán implementace.

Plán implementace:

- Analýza, konzultace a návrh vhodného harmonogramu implementace
- Pilotní nasazení
- Školení správců, dokumentace
- Workshop pro techniky a uživatelskou podporu
- Workshop, webinář, nebo on-line kurz pro uživatele
- 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 multifaktorové autentizace (MFA) v prostředí OU
- 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 **pilotního nasazení** multifaktorové autentizace se všemi zmíněnými požadavky (pro vymezené testovací skupiny uživatelů)
- Návrh **nasazení multifaktorové autentizace** 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)
- 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 obsahovat 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** multifaktorové autentizace 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** (administrátorské konzole v rámci prostředí Microsoft 365, Entra a návazných platforem týkající se správy a nastavení multifaktorové autentizace a jejího zabezpečení, reakce na bezpečnostní incidenty, auditu, troubleshootingu, postupného škálování a rozšiřování atd.)
- **Provozní dokumentace**, popis konfigurací a postupů včetně možnosti postupného škálování a popisu řešení obvyklých potenciálních problémů jako jsou bezpečnostní postupy v případě kompromitace uživatele, ztráty nebo zapomenutí autentizačního faktoru, registrace nebo resetu autentizačního faktoru atd. Rozsah dokumentace musí odpovídat komplexitě a rozmanitosti zadání
- Návody pro techniky (návody na nastavení multifaktorové autentizace reflektující implementované škálování, návody na běžné troubleshooting situace jako jsou ztráty a zapomenutí autentizačních faktorů atd.)
- Workshop, webinář, nebo on-line kurz pro uživatele
- 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
- 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 dodány 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 MFA, 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 se správci CIT

6. Závěry

Implementace multifaktorové autentizace 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.