TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta mechatroniky, informatiky
a mezioborových studií

Integrace MS Azure v komerční firmě

Bakalářská práce

Studijní program: B2612 Elektrotechnika a informatika
Studijní obor: Informatika a logistika (P)

Autor práce: **Michal Danda**
Vedoucí práce: Ing. Leoš Petržílka
Ústav informačních technologií a elektroniky

TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta mechatroniky, informatiky
a mezioborových studií

Zadání bakalářské práce

Integrace MS Azure v komerční firmě

Jméno a příjmení: **Michal Danda**
Osobní číslo: M17000185
Studijní program: B2612 Elektrotechnika a informatika
Studijní obor: Informatika a logistika
Zadávající katedra: Ústav informačních technologií a elektroniky
Akademický rok: **2019/2020**

Zásady pro vypracování:

1. Seznamte se s platformami MS Office 365 a MS Azure.
2. Analyzujte a zhodnoťte aktuální stav implementace z pohledu procesů, nákladů a zabezpečení.
3. Navrhněte a realizujte změny v implementaci vyplývající z provedené analýzy.
4. Pro navrženou implementaci definujte optimální množinu zásad v modulu Azure Policy.

Rozsah grafických prací:	dle potřeby dokumentace
Rozsah pracovní zprávy:	30-40 stran
Forma zpracování práce:	tištěná/elektronická
Jazyk práce:	Čeština

Seznam odborné literatury:

[1] Get started with Azure [online]. Redmond, Washington, 2019 [cit. 2019-10-16]. Dostupné z: https://docs.microsoft.com/en-us/azure/#pivot=get-started&panel=get-started1
[2] Microsoft Docs [online]. Redmond, Washington, 2019 [cit. 2019-10-16]. Dostupné z: https://docs.microsoft.com/en-us/

Vedoucí práce:	Ing. Leoš Petržílka Ústav informačních technologií a elektroniky
Datum zadání práce:	9. října 2019
Předpokládaný termín odevzdání:	18. května 2020

L.S.

prof. Ing. Zdeněk Plíva, Ph.D.
děkan

prof. Ing. Ondřej Novák, CSc.
vedoucí ústavu

V Liberci dne 18. října 2019

Prohlášení

Prohlašuji, že svou bakalářskou práci jsem vypracoval samostatně jako původní dílo s použitím uvedené literatury a na základě konzultací s vedoucím mé bakalářské práce a konzultantem.

Jsem si vědom toho, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci nezasahuje do mých autorských práv užitím mé bakalářské práce pro vnitřní potřebu Technické univerzity v Liberci.

Užiji-li bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti Technickou univerzitu v Liberci; v tomto případě má Technická univerzita v Liberci právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Současně čestně prohlašuji, že text elektronické podoby práce vložený do IS/STAG se shoduje s textem tištěné podoby práce.

Beru na vědomí, že má bakalářská práce bude zveřejněna Technickou univerzitou v Liberci v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů.

Jsem si vědom následků, které podle zákona o vysokých školách mohou vyplývat z porušení tohoto prohlášení.

28. května 2020 Michal Danda

Poděkování

Rád bych poděkoval vedoucímu mého bakalářského projektu Ing. Leoši Petržílkovi, konzultantce z hlediska analýzy a ekonomiky Ing. Julii Mokré, Ph.D., a konzultantovi Michalu Čermákovi za poskytnutí odborných rad, ochotu a vstřícný přístup během celé práce na dané problematice.

Abstrakt

Cílem práce je seznámení se s platformami cloudových služeb Microsoft Office 365 a Microsoft Azure, které následuje analýza aktuálního stavu zvoleného subjektu a vytyčení bodů optimalizací a změn a jejich následná implementace. Vše především z pohledu efektivity procesů a zabezpečení. Výstupem práce je definice zásad Azure Policy pro správné řízení zmíněných služeb.

Klíčová slova

Cloudová řešení, Office, Microsoft, Azure, SharePoint Online, řízení firmy

Abstract

Focus of this thesis is to get to know features and functions of Microsoft Office 365 and Microsoft Azure platform in commerical environment, which is followed by an analysis of the current state of the selected entity and setting points for optimizations and changes and their subsequent implementation. All from the point of view of process efficiency and security. The output of the work is the definition of Azure Policy for the proper management of these services.

Key Words

Cloud solution, Office, Microsoft, Azure, SharePoint Online, company management

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých symbolů a zkratek

MS – Microsoft

AIP – Azure Information Protection

IoT – Internet of Things

SaaS – Software as a Service

IaaS – Infrastructure as a Service

VM – Virtual Machine

Úvod

Vlastní infrastruktura ve formě serverů a rozsáhlých datových úložišť je v dnešní době rychlého internetového připojení a cloudu již zastaralý model řešení. Alespoň pro malé firmy, které potřebují investovat jinde než do drahého a na údržbu náročného hardwaru. Naproti tomu model firmy v cloudu přináší nesčetně mnoho výhod. Tam, kde bylo dříve nutné koupit nová disková pole, stačí dnes pouze „přejet posuvníkem“ a rozšířit kapacitu během pár minut.

Cílem této práce je implementovat cloudovou platformu Microsoft Azure do prostředí malé firmy. Z celé škály cloudových řešení, jako je Amazon Web Services, Google Suite a podobně, bylo vybráno Microsoft Azure, protože firma již používá software od firmy Microsoft a využít jinou platformu by již nebylo praktické.

Tato práce je rozdělena do tří částí. První část se zabývá teoretickým seznámením s relevantními aplikacemi a službami Azure a také MS Office 365. V této části jsou také zmíněny licenční podmínky, které jsou poměrně rozsáhlé.

Druhá část se věnuje analýze aktuálního stavu z hlediska využívaných aplikací, služeb a licencí. Dále jsou zde stanoveny kritické body informačního systému firmy a stanoveny obecné možnosti optimalizace, a to i z hlediska financí, hned v několika modelech.

Třetí část se věnuje praktické implementaci vybraných služeb a modulů Azure, které vyplývají z předchozí analýzy. Implementace těchto služeb je ukázána na vzorových příkladech. V této části bakalářská práce definuje množinu zásad a pravidel (Policies), která ustanovuje chování implementovaných aplikací a služeb Azure. Firmě tak umožní požadované, jednoznačné a bezpečné nakládání s dokumenty a informacemi.

Závěrem práce je pak shrnutí aktuálního stavu integrace, porovnání kritických bodů informačního systému s výsledky implementace a shrnutí nejdůležitějších zásad.

1 Seznámení s Microsoft Azure a Office 365

Microsoft Azure představuje soubor stovek infrastrukturních, platformních a cloudových služeb, integrovaných do zákaznického portálu. Tento veřejný cloud je provozován společností Microsoft.

Microsoft Office 365 je výkonný a rozsáhlý balík cloudových služeb a kancelářského softwaru.

1.1 Úvod do MS Azure a cloud computingu

Historie Microsoft Azure se začala psát v polovině roku 2000 jako interní iniciativa s názvem „Project Red Dog“. V té době již Amazon spustil službu cloud computing a Microsoft potřeboval odpovědět. (1)

Během konference Microsoft Professional Developers Conference v roce 2008, dva roky poté, co Amazon Web Services (AWS) uvedla do provozu svou Simple Storage Service, společnost Microsoft, oznámila, že plánuje zahájit vlastní cloud computingovou službu s názvem Windows Azure. Plán společnosti Microsoft byl nabídnout pět hlavních kategorií cloudových služeb:

- Windows Azure pro výpočetní, úložiště a vytváření sítí;
- Služby Microsoft SQL pro databáze;
- Služby Microsoft .NET pro vývojáře;
- Life Services pro sdílení souborů;
- Microsoft SharePoint Services a Microsoft Dynamics CRM Services SaaS. (1)

Po oznámení počátku vývoje začal Microsoft postupně vydávat testovací verze různých služeb s tím, že v únoru roku 2010 se platforma Windows Azure stala komerčně dostupnou službou. Po počátečních smíšených reakcích přišlo mnoho zásadních vylepšení a v roce 2014 se již služba posunula daleko za Windows a byla přejmenována na Microsoft Azure. (1)

Microsoft Azure je cloudová platforma, která umožňuje přístup k serverům, aplikacím, úložištím nebo software přes internet. Platformy cloud computingu jako je Azure jsou levnější, bezpečnější, spolehlivější, a hlavně flexibilnější než vlastní servery umístěné například ve firmě. Je možné si z něho vybrat a používat jakékoli části, také lze velice rychle měnit velikosti úložiště či výpočetní výkon. Nabízené výpočetní služby mají tendenci se podle poskytovatele cloudových služeb lišit. Většinou ale zahrnují: (2)

- **Výpočetní výkon** – například linuxové servery nebo webové aplikace
- **Úložiště** – například soubory a databáze
- **Sítě** – například zabezpečená připojení mezi poskytovatelem cloudu a vaší společnosti
- **Analýzu** – například vizualizaci telemetrických a výkonnostních údajů

Cloud computing je pronájem prostředků, například úložného prostoru nebo výkon procesoru. Firma poskytující tyto služby se označuje jako poskytovatel cloudu. Příkladem takových poskytovatelů je Microsoft, Amazon a Google. (2)

Cloud computing nepředstavuje přístup ke službám typu „všechno nebo nic“. Společnosti se mohou rozhodnout, do jaké míry budou používat cloudové služby a do jaké míry vlastní infrastrukturu. Existující firmy můžou zvolit postupný přechod ke cloudu, aby ušetřily náklady na infrastrukturu a správu, zatímco nové společnosti můžou začít rovnou s cloudem. (2)

1.2 Úvod do Microsoft Office 365

Office 365 vyniká jednoduchou týmovou komunikací, výměnou souborů, spoluprací na projektech a propojením samostatných softwarových nástrojů s cloudovými službami. (3)

Kromě známých kancelářských aplikací, jako Word, Excel, OneNote, jsou součástí balíku Microsoft Office 365 také groupwarové – týmové aplikace nebo aplikace pro ukládání dat. Přehled nejdůležitějších aplikací:

- **Teams** – poskytují trvalou komunikační metodu založenou na chatu, která umožňuje oddělit konverzaci založenou na tématech podle kanálu. (4)
- **Outlook** – není pouze e-mailový klient, obsahuje také diář a zjednodušené skupiny pro týmovou spolupráci. (5)
- **SharePoint Online** – slouží k vytváření webů organizací. Lze ho používat pro ukládání, uspořádání a sdílení informací a přístup k nim z libovolného zařízení přes webový prohlížeč. Vytváří pro každou skupinu vlastní kolekci či web. (6)
- **OneDrive** – je cloudové úložiště, k datům má uživatel přístup ze všech svých zařízení. Díky OneDrive jsou data neustále synchronizována. Také je propojen se službou SharePoint Online, která využívá OneDrive k synchronizaci dat z webů SharePoint Online, která jsou uložená v zařízení. (5)
- **Planner** – je součástí Teams, je využíván pro plánování úkolů, jsou zde tvořeny úkoly pro jednoho či více lidí.

1.3 Přehled cloudových služeb Azure (1)

Microsoft Azure nabízí extrémně velké portfolio cloudových služeb. Některé služby jsou přímo pod Azure, některé jsou poskytované i zvlášť, nicméně se často překrývají. Význam jednotlivých služeb:

- **Management and Governance** – automatizace a optimalizace správy a dodržování předpisů cloudových prostředků, zahrnuje například Azure Backup, Azure Advisor, Scheduler, Automation, Azure Policy
- **Blockchain** – kompilace a správa blockchainových aplikací s využitím sady integrovaných nástrojů
- **Developer Tools** – sestavování, správa a průběžné doručování cloudových aplikací, a to na jakékoli platformě a v jakémkoli jazyce
- **Compute** – přístup ke cloudové výpočetní kapacitě a škálování na vyžádání, zahrnuje například Virtual Machines, Virtual Machine Scale Sets, Azure Kubernetes Service (AKS) a Cloud Services for building cloud-based apps and APIs

- **Networking** – propojení cloudových a místních infrastruktur a služeb uživatele zahrnuje řadu síťových nástrojů, jako je virtuální síť, která se může připojit k datovým centrům na místě, zahrnuje například Load Balancer, Application Gateway, VPN Gateway, Azure DNS for domain hosting, Content Delivery Network, Traffic Manager
- **Storage** – zajištění zabezpečeného a rozsáhle škálovatelného cloudového úložiště pro data, aplikace a úlohy, zahrnuje mimo jiné úložiště Blob, File and Disk Storage, také Data Lake Store, Backup and Site Recovery
- **Web** – rychlé a efektivní sestavování, nasazování a škálování výkonných webových aplikací, zahrnuje například App Service, Azure Maps, Web Apps, API Apps
- **Mobile** – zahrnuje několik služeb pro vytváření a nasazení aplikací, ale nejzajímavější je pravděpodobně App Service, která zahrnuje služby pro Web Apps, Mobile Apps, Logic Apps a API Apps (pro vytváření a používání API)
- **Containers** – rychlejší vývoj a správa kontejnerizovaných aplikací pomocí integrovaných nástrojů
- **Databases** – zahrnuje několik databází založených na SQL a souvisejících nástrojů, jakož i Cosmos DB, tabulkový úložiště pro NoSQL a technologii Redis Cache in-memory
- **Data + Analytics** – shromažďování, ukládání, zpracování, analýza a vizualizace dat jakéhokoli druhu, objemu nebo rychlosti
- **AI + Machine Learning** – zahrnuje několik nástrojů pro vývoj aplikací s umělou inteligencí, jako je například rozhraní Computer Vision, Face API, Bing Web Search, Video Indexer, Intelligent Service pro porozumění jazyku a další
- **Internet of Things** – zahrnuje služby IoT Hub a IoT Edge, které lze kombinovat s celou řadou strojového učení, analytických a komunikačních služeb
- **Enterprise Integration** – zahrnuje více nástrojů pro vytváření a správu hybridních cloud computingových prostředí
- **Security** – zahrnuje Security Center, Azure Active Directory, Key Vault and Multi-Factor Authentication Services

- **Microsoft Azure Stack** – zahrnuje řešení pro replikaci infrastruktury Azure v podnikových datových centrech s cílem usnadnit hybridní cloudové nasazení
- **Hybrid** – inovace Azure a flexibilita a rychlé inovace cloud computingu pro úlohy ve vašem místním prostředí
- **Identity** – správa identit uživatelů a přístupu k ochraně před pokročilými hrozbami napříč zařízeními, daty, aplikacemi i infrastrukturou
- **Media** - zajištění vysoce kvalitního audiovizuálního obsahu kdekoli, kdykoli a na libovolném zařízení
- **Migration** – zjednodušení a zrychlení migrace do cloudu s pokyny, nástroji a prostředky
- **Mixed Reality** - zjednodušení, automatizace a optimalizace správy a dodržování předpisů cloudových prostředků
- **Windows Virtual Desktop** – sestavování, správa a průběžné doručování cloudových aplikací na jakékoli platformě a v jakémkoli jazyce (1)

1.4 Rozšíření Enterprise Mobility + Security

Enterprise Mobility + Security (zkráceně EMS) rozšiřuje zabezpečení Office 365. Některé bezpečnostní funkce modulu EMS se s vlastním zabezpečením Office365 překrývají, jiné nabízejí širší a komfortnější nastavení, umožňují kombinovat zásady s jinými službami a výrazněji podporují mobilitu služeb, procesů i zpracovávaných dokumentů. EMS obsahuje několik služeb pro zabezpečení: (7)

- Azure Active Directory
- Microsoft Intune
- Microsoft Endpoint Congfiguration Manager
- Microsoft Cloud App Security
- Azure Information Protection
- Microsoft Identity Manager
- a další…

Poměrně důležitá je služba Microsoft Intune, která spravuje mobilní zařízení, aplikace a počítače z cloudu. Dále pak Microsoft Endpoint Configuration Manager, který spravuje místní počítače, servery a mobilní zařízení s využitím cloudových přehledů. (7)

1.5 Důležité moduly z hlediska zabezpečení

Jak již bylo několikrát zdůrazněno, rozhodujícím kritériem analýzy a implementace cloudových služeb Azure je bezpečnost a efektivita zpracovávaných procesů. Z tohoto pohledu se jeví jako nejužitečnější následující moduly.

1.5.1 Modul Management and Governance

Obsahuje integrované nástroje pro správu a řízení Azure, které správcům systémů a vývojářům pomáhají zajistit zabezpečení a dodržování předpisů vašich prostředků v místním prostředí i v cloudu. V průběhu celého životního cyklu IT je možné monitorovat infrastrukturu a aplikace, zřizovat a konfigurovat prostředky, aktualizovat aplikace, analyzovat hrozby, zálohovat prostředky, vytvářet řešení zotavení po havárii, používat zásady, automatizovat procesy, a dokonce i spravovat náklady. (8)

Tabulka 1: Nástroje pro správu určené k monitorování (8)

Nástroje pro správu určené k monitorování:	
Azure Monitor	Přehled o stavu komponent platformy Azure
Log Analytics	Shromažďování, vyhledávání a vizualizace počítačových dat z místních počítačů a cloudu
Network Watcher	Monitorování a diagnostika problémů se sítí

Tabulka 2: Nástroje pro správu určené ke konfiguraci (8)

Nástroje pro správu určené ke konfiguraci:	
Automation	Automatizace, konfigurace a aktualizace prostředků
Azure Advisor	Získejte individuální doporučení, která vám pomůžou se správou prostředí Azure
Azure Resource Manager	Nasazování a správa prostředků Azure
Scheduler	Vytváření, údržba a vyvolávání naplánované práce pro aplikace
Traffic Manager	Směrování příchozího provozu pro zajištění vyššího výkonu a dostupnosti
Cloud Shell	Správa Azure pomocí prostředí příkazového řádku
Azure Managed Applications	Správa nasazených řešení pro zákazníky
Microsoft Azure Portal	Přizpůsobení a správa prostředí Azure
Mobilní aplikace Azure	Stálé připojení k prostředkům Azure kdykoli a odkudkoli

Tabulka 3: Nástroje pro správu určené pro zásady řízení (8)

Nástroje pro správu určené pro zásady správného řízení:	
Správa nákladů a fakturace	Získání transparentního přehledu o nákladech na cloudové prostředky
Azure Policy	Nastavení zásad napříč prostředky a monitorování dodržování předpisů
Azure Blueprint	Možnost rychlého a opakovatelného vytváření řízených prostředí

Tabulka 4: Nástroje pro správu určené k zabezpečení a ochraně (8)

Nástroje pro správu určené k zabezpečení a ochraně:	
Azure Backup	Zálohování prostředků a ochrana před ztrátou dat
Azure Site Recovery	Doručování vysoce dostupných virtuálních počítačů s integrovaným zotavením po havárii
Security Center	Zabezpečení prostředků a ochrana před hrozbami

1.5.2 Modul Identity

Správa identit a řízení přístupu. Obrana před škodlivými pokusy o přihlášení a ochrana přihlašovacích údajů s použitím řízení přístupu na základě rizikových událostí, nástrojů pro ochranu identity a výkonných možností ověřování. (9)

Tabulka 5: Nástroje pro správu identit a řízení přístupu (9)

Nástroje pro správu identit a řízení přístupu:	
Azure Active Directory	Zajištění správy identit a řízení přístupu pro cloudová a hybridní prostředí
Azure Active Directory B2C	Správa a ochrana identit zákazníků a přístupu v cloudu s použitím funkcí zabezpečení IAM
Azure Active Directory Domain Services	Připojení virtuálních počítačů v Azure k doméně bez nasazení řadičů domény

1.5.3 Modul Security

Zabezpečení cloudových úloh použitím integrovaných služeb. Integrované služby zabezpečení v Azure, včetně inteligentního zabezpečení, které pomáhá včas identifikovat rychle se vyvíjející hrozby, umožňují chránit data, aplikace i infrastrukturu. Strategie vícevrstvé bezpečnosti (defense-in-depth) napříč identitami, daty, hostiteli a sítěmi. Zajištění jednotné správy zabezpečení a pokročilé ochrany před hrozbami napříč hybridními cloudovými prostředími. (10)

Tabulka 6: Nástroje pro správu určené k zabezpečení a ochraně (10)

Nástroje pro správu určené k zabezpečení a ochraně:	
Security Center	Zajištění jednotné správy zabezpečení a pokročilé ochrany před hrozbami pro úlohy v cloudu i lokálním prostředí
Key Vault	Ochrana kryptografických klíčů a dalších tajných kódů používaných cloudovými aplikacemi a službám
Azure DDoS Protection	Ochrana prostředků Azure před hrozbami odepření služeb
Azure Information Protection	Kontrola nad e-maily, dokumenty a citlivými daty sdílenými mimo vaši společnost a pomoc s jejich zabezpečením
Application Gateway	Ochrana aplikací před běžným webovým ohrožením a zneužitím díky integrovanému firewallu webových aplikací

1.6 Licenční podmínky

Licenční politika Azure je poměrně rozsáhlá a složitá, služby lze získat na základě celých licenčních balíků, tak i jednotlivě, avšak méně výhodně. Dále pak samotný computing lze vypočítat podle cenové kalkulačky na webu Azure, kde lze navolit například počet virtuálních počítačů, dobu používání, operační systém, výkon apod., následně dostanu výslednou cenu. Hodí se podotknout, že ceny za licence nejsou dány pevně, lze si dohodnout cenu při kontaktovaní obchodního oddělení.

Licence je tedy možně rozdělit do několika kategorií:

- Součást Microsoft 365 pro firmy
- Součást Microsoft 365 pro podniky
- Azure Active Directory
- Enterprise Mobility + Security
- Samostatné služby
- Cenová kalkulačka

1.6.1 Licence Azure jako součást Microsoft 365 pro firmy

Mezi licencemi pro firmy jsou poměrně zásadní rozdíly, nejnižší licence neobsahuje ani desktopové verze aplikací Office 365, zatímco nejvyšší licence již obsahuje poměrně zajímavé možnosti týkající se Azure a zabezpečení, jako například Intune. Licence Microsoft 365 Business Standard i Microsoft 365 Business Premium nabízejí Azure Active Directory. V tabulce jsou zmíněny jen některé nejzásadnější služby nebo funkce, kompletní výčet by byl moc dlouhý. (11)

Tabulka 7: Porovnání licencí Microsoft 365 pro firmy (11)

Licence	**Microsoft 365 Business Basic**	**Microsoft 365 Business Standard**	**Microsoft 365 Business Premium**
Cena (měsíc/uživatel)	€4.20	€10.50	€16.90
Popis:	Web verze aplikací Office, Email, Kalendáře, Týmový práce, Ukládaní sdílení souborů, Zabezpečení a dodržování předpisů	Web verze aplikací Office, Email, Kalendáře, Týmový práce, Ukládaní sdílení souborů, Zabezpečení a dodržování předpisů, Desktop verze aplikací Office	Web verze aplikací Office, Email, Kalendáře, Týmový práce, Ukládaní sdílení souborů, Zabezpečení a dodržování předpisů, Desktop verze aplikací Office, Pokročilé zabezpečení, Správa zařízení
Souvislost s Azure:	Licence Azure AD FREE	Licence Azure AD Office 365 Apps	Licence Azure AD Office 365 Apps, MS Intune

1.6.2 Licence Azure jako součást Microsoft 365 pro podniky

Licence pro podniky jsou zde brány z plánu Enterprise, existuje i další, širší plán, ale ten by nebyl relevantní pro použití v této práci. Následující licence obsahují podobně jako v licence v předchozí kapitole základní kancelářské a týmové aplikace, k nim se ovšem přidává poměrně široké portfolio další samostatných licencí. Licence E5 obsahuje v podstatě vše, co Microsoft nabízí, kompletní portfolio aplikací, služeb. Licence E3 je o něco omezenější. V tabulce jsou zmíněny jen některé nejzásadnější služby nebo funkce, kompletní výčet by byl moc dlouhý. (12)

Tabulka 8: Porovnání licencí Microsoft 365 pro podniky (12)

Licence	**Microsoft 365 E3**	**Microsoft 365 E5**
Cena (měsíc/uživatel)	€19.70	€34.40
Popis:	Operační systém, web verze aplikací Office, Email, Kalendáře, Týmový práce, Ukládaní sdílení souborů, Zabezpečení a dodržování předpisů, Desktop verze aplikací Office	Operační systém, web verze aplikací Office, Email, Kalendáře, Týmový práce, Ukládaní sdílení souborů, Zabezpečení a dodržování předpisů, Desktop verze aplikací Office, Pokročilé zabezpečení, Správa zařízení
Souvislost s Azure:	Azure Active Directory Premium 1, Microsoft Intune, Azure Information Protection P1	Azure Active Directory Premium 1,2, Microsoft Intune, Azure Advanced Threat Protection, Azure Information Protection P1, P2

1.6.3 Licence Azure Active Directory

Azure Active Directory existuje v několika verzích, nižší verze jsou obsaženy v licencích Microsoft 365, za vyšší verze je nutné zaplatit. Pouze licence pro podniky Microsoft 365 E5 obsahuje nejvyšší verzi Azure Active Directory a tím není nutné si ji platit zvlášť. Edice Free je součástí předplatných pro komerční online služby, jako jsou Azure, Dynamics 365, Intune a Power Platform. Dostupné verze: (13)

Tabulka 9: Porovnání licencí Azure Active Directory (13)

Licence	Free	Apps Office 365	Premium P1	Premium P2
Cena nebo licence:	zdarma	MS365, E1, E3, E5	E3, E5, jinak €5.06	E5, jinak €7.59
Obsahuje:	Základní nástroje pro správu identit a přístupu, omezený počet objektů	Základní nástroje pro správu identit a přístupu, některé rozšířené možnosti zabezpečení	Obsahuje všechny funkce jako licence Apps Office 365 a tomu široké možnosti automatizace procesů	Obsahuje vše, co licence P1 a navíc rozšířenou ochranu identit a možnosti správy privilegovaných identit.

1.6.4 Licence pro Enterprise Mobility + Security

Modul pro zabezpečení Enterprise Mobility + Security je možné koupit jako samostatné licence, nebo je obsažen částečně nebo i celý v licenci pro podniky. Tabulka obsahuje pouze nejrelevantnější informace pro použití v této práci, kompletní výčet by byl moc dlouhý. (14)

Tabulka 10: Porovnání licencí Enterprise Mobility + Security (14)

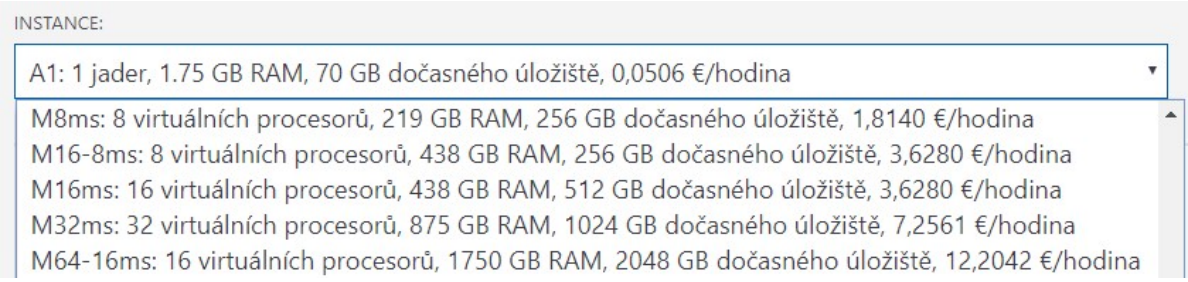
Licence	Enterprise Mobility + Security E3	Enterprise Mobility + Security E5
Cena(měsíc/uživatel):	€7.40	€12.50
Obsahuje:	Správa identit a přístupů, ochrana informací, zabezpečení založené na identitách	Obsahuje vše, co licence E3, a navíc rozšířené možnosti správy identit a přístupů a také rozšířenou ochranu informací
Důležité součásti pro Azure:	Microsoft Advanced Threat Analytics	Azure Advanced Threat Protection, Služba Privileged Identity Management

1.6.5 Cenová kalkulačka

Jak již bylo zmíněno v přechozích kapitolách, Azure nabízí kromě služeb, také prostředky, například úložný prostor, výkon procesoru nebo virtuální počítače. Všechny tyto prostředky jsou škálovatelné a platí se podle toho, do jaké míry jsou využívány. Například cena virtuálních počítačů je závislá na množství, hodinách, výkonu apod. K výpočtu přibližné ceny slouží cenová kalkulačka, pomocí které lze stanovit po zadání vlastních parametrů přibližnou cenu. Tato kalkulačka se nachází přímo na webových stránkách Microsoft Azure.

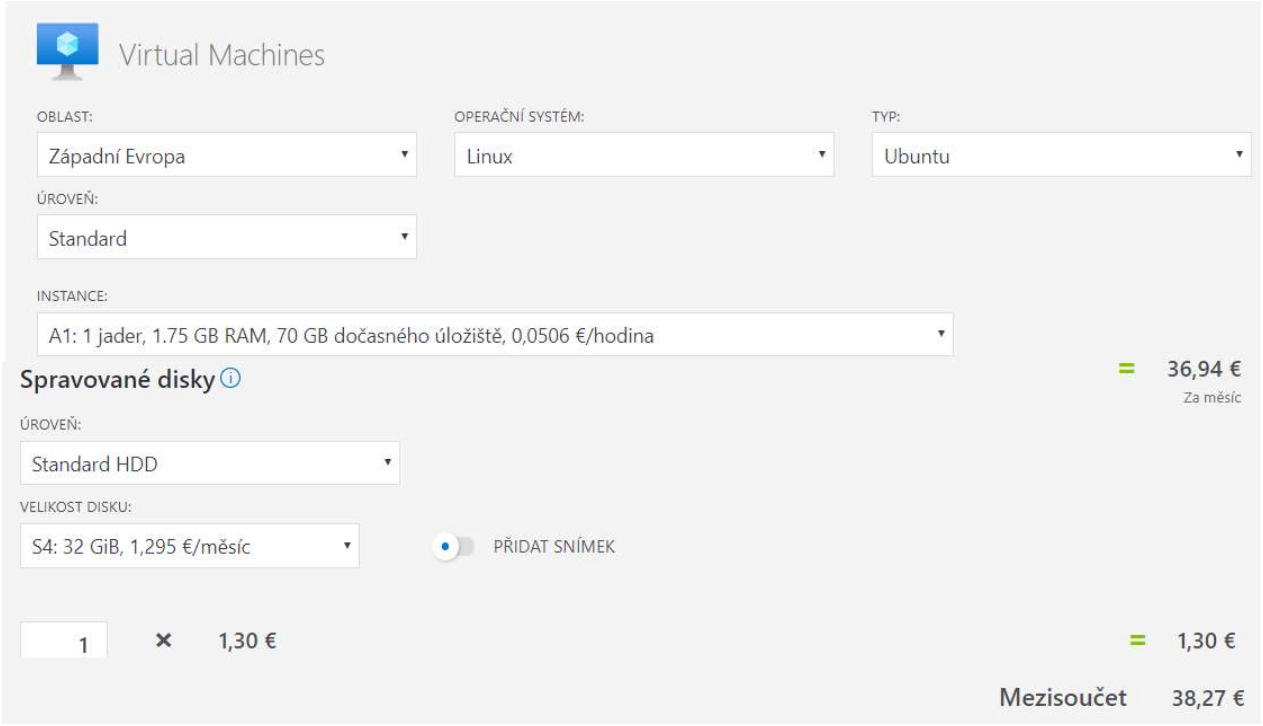
Virtuální počítače

Cenová kalkulačka nabízí několik desítek možností podle potřebného výkonu, paměti a podobně. Lze tedy virtuální počítač optimalizovat pro jednoduchou webovou aplikaci, tak i pro strojové učení. Na následujícím obrázku je ukázka několika konfigurací procesorů a pamětí i s cenami za hodinu provozu. Jak je vidět, je zde opravdu široká výkonová škála. (15)



Obrázek 1: Hardwarové sestavy u VM (15)

Na následujícím obrázku je ukázka části cenové kalkulačky pro virtuální stroje. Pro příklad je nakonfigurován počítač, který by splňoval požadavky pro běh jednoduché webové aplikace na Linuxu. Dále je zde možné vybrat z několika různých linuxových distribucí. Další možností je také volba disků, kde je možné nakonfigurovat jak HDD, tak i SDD disky. Zde jsou samozřejmě zásadní rozdíly v ceně. (15)



Obrázek 2: Cenová kalkulačka u VM (13)

K virtuálním počítačům je možné také zakoupit podporu v několika licencích. Rozdíly mezi standardní a prémiovou podporou jsou v řádu stovek eur.

SQL Database

SQL databáze lze nakonfigurovat obdobným způsobem jako virtuální počítače. Jsou zde desítky různých možností, z kterých je následně vypočítána cena. Cena databáze pro obecné využití, bez zvýšené ochrany dat, s možností zpětného obnovení k určitému okamžiku, týdenní uchování záloh a 200 GB prostoru je vypočítána na 37.11€ za měsíc. (16)

Další možnosti

Kromě dvou předchozích příkladů je možné tímto způsobem navolit desítky dalších služeb či prostředků Azure. Pomocí kalkulačky lze nakonfigurovat i rozsáhlé scénáře s desítkami různých služeb.

2 Analýza zvoleného subjektu

Nevyhnutelným předpokladem pro správnou implementaci zamýšlených služeb je kvalitní analýza současného stavu. Měla by respektovat všechny možnosti a nápady firmy, porovnávat současné varianty řešení ale také například zahrnout finanční situaci firmy.

2.1 Analýza aktuálního stavu

Licence a služby Microsoft

Firma, která je předmětem této práce, má 13 zaměstnanců. Aktuálně mají někteří zaměstnanci nižší licence Office 365 Essential a někteří střední licence Office 365 Business Premium. Licence Essential nemají ani desktopové verze Office kancelářského balíku. Prozatímně je to řešeno přihlášením se na daný počítač s nižší licencí, účtem někoho s vyšší licencí. Microsoft Azure je aktuálně využit jen pro správu Active Directory, což je zdarma k licencím Office 365.

Ve firmě jsou do značné míry využívány již implementované aplikace z balíku Microsoft Office 365. Kromě kancelářského softwaru Office, jsou to hlavně Microsoft Teams, SharePoint Online. Veškeré soubory či dokumenty jsou sdílené na SharePoint weby. Složky na SharePoint webu jsou také namapovány v soukromých úložištích, což značně ulehčuje a zjednodušuje práci, nicméně přináší i rizika.

Velikost firemního cloudového úložiště je standardní 1 TB, což je součástí licencí Office 365 Business Premium, kromě toho má každý uživatel na svém uložišti OneDrive 1 TB místa. (11)

Účetní systém

Dále je zde účetní systém, řešený na základě platformy iPodnik, který poskytuje server hosting a SQL databázi. Na server hostingu následně běží účetní systém Altus Vario. Na server se musí přistupovat přes vzdálenou plochu a platí se za každého uživatele, který má svůj účet. Aktuálně mají přístup do účetnictví čtyři lidé, včetně externí účetní. Tento systém je značně nepohodlný, protože ani admin z pohledu naší firmy, nemá práva na hostingu například aktualizovat software a vše je poměrně pomalé. Další nevýhodou je nemožnost pracovat se systémem offline.

Webový hosting

Větší pozornost a péči by zasloužil také firemní web. Stránka je prozatím statická, bez nároků na výpočetní výkon, je hostovaná na externím serveru.

Shrnutí nákladů souvisejících se softwarem

Tabulka níže shrnuje aktuální stav licencí a dalšího pronajímaného softwaru a náklady na tyto služby.

Tabulka 11: Aktuální náklady související se softwarem

Aktuální náklady související se softwarem				
Položka	**Měrná jednotka**	**Jednotková cena**	**Počet měr. Jednotek**	**Kalkulovaná cena měsíc**
Licence MS Office 365 Essentials	Kč za měsíc/licence	105,00	6	630,00 Kč
Licence MS Office 365 Premium	Kč za měsíc/licence	262,50	7	1 837,50 Kč
IPodnik – základ	Kč/měsíc	302,50	4	1 210,00 Kč
Server hosting pro účet. sys. IPodnik	Kč/měsíc	205,50	4	822,00 Kč
SQL DB Server Express pro účet. sys.	Kč/měsíc	435,00	1	435,00 Kč
Hosting webové stránky	Kč/rok	42,00	1	42,00 Kč
			Celkem za měsíc:	4 976,50 Kč
			Celkem za rok:	59 718,00 Kč

2.2 Kritická místa v informačním systému firmy

Zabezpečení citlivých dokumentů

Jedním z kritických míst v zabezpečení je ochrana interních dokumentů. Ve firmě se pracuje s citlivými dokumenty, týkající se financí, obchodních nabídek a podobně. Tyto dokumenty je třeba chránit tak, aby nedošlo ke chtěnému nebo nechtěnému úniku dat, který by měl za následek poškození firmy.

Správa a kontrola nad firemním hardwarem

Vzhledem k zaměření firmy na IT a software, má každý zaměstnanec služební notebook a služební telefon. Tato zařízení nejsou pod kontrolou a v případě ovládnutí, hrozí ztráta dat, případně i ovládnutí celého uživatelského účtu. V případě ovládnutí účtu správce mohou nastat velké škody.

Konfigurace nového hardwaru

S každým novým zaměstnancem přibývá také nový počítač. Ten je nutné alespoň základním způsobem nakonfigurovat, stáhnout potřebný software, vývojová prostředí pro programování, různé specializované ovladače pro konkrétní použití. Takovéto rutinní nastavení a konfigurace zabere spoustu času, instalace některého specializovaného softwaru může zabrat celý den.

Omezené cloudové úložiště

Velikost cloudového úložiště je omezena na 1 TB, což se v poslední době stává silně nedostačující. Úložiště je již ze 70 % zaplněno.

Zálohování dat

Celé firemní cloudové úložiště je nepravidelně zálohované na on-premise úložiště NAS (datové úložiště připojené k místní síti) manažera firmy. Toto zálohování je ovšem prováděno manuálně, nepravidelně a nelze držet více než 2 poslední zálohy. I přesto, že je Microsoft OneDrive spolehlivé úložiště, stejně je požadavek, aby byla data ještě zálohována na externí úložiště.

Nejednotnost v AD

Obecně panuje zmatek v Active Directory, problémem jsou nejednotné názvy zařízení, nejednotná konfigurace, to poté působí problémy s další konfigurací.

Účetní systém

Výše zmiňovaný účetní systém, který je hostovaný na externím serveru a přistupuje se k němu přes vzdálenou plochu, představuje značný problém a zpomaluje interní procesy ve firmě.

2.3 Obecně možná řešení

Firma má v plánu využít služeb Azure zejména při zlepšení zabezpečení svých administrativních procesů. Aktuálně využívané licence nedávají příliš mnoho prostoru k vylepšení zabezpečení. Z hlediska zabezpečení je nejdostupnější služba Intune, která spravuje mobilní zařízení, aplikace a počítače z cloudu. Dále potom Azure Information Protection (AIP), které organizaci pomáhá klasifikovat a volitelně chránit své dokumenty a e-maily použitím popisků. Další možností zabezpečení je modul Enterprise Mobilit + Security. Tento modul je zaměřen pouze na zabezpečení. EMS zároveň obsahuje a rozšiřuje Intune i AIP, zmíněné služby jsou součástí licence Microsoft 365 Business.

Pro zálohování na externí úložiště je nutné koupit nové úložiště nebo rozšířit současnou NAS, poté využít službu Azure pro zálohování.

Účetnictví je závislé na systému Altus Vario, který hostuje platforma iPodnik na svém serveru spolu s databází. Možnosti pro hosting, přístup a databázi Azure nabízí také. Azure SQL Database lze využít jako škálovatelnou databázi pro účetní systém. Pro hosting je možné použít službu Virtual Machines nebo Windows Virtual Desktop, pod kterým může mít firma plnou kontrolu s neomezeným přístupem na rozdíl od hostovaných serverů.

Pro hostování webové stránky lze využít službu Azure App Service, kde je možné zvolit požadované vlastnosti, jako operační systém a výkon.

3 Kalkulace nákladů a nákladové modely

Tato kapitola se bude věnovat kalkulaci nákladů podle různých možností licencí, zakoupených služeb Azure a podobně.

3.1 Nákladové modely Azure

Zde budou uvedeny tři modely, které se liší cenou i použitými licencemi a také možnostmi nákupu hardwaru pro zálohování. Ve všech modelech bude také započítána mzda za čas strávený implementací Azure, toto bylo odhadnuto na 100 hodin. Modely:

1. Minimální investice
2. Střední investice
3. Velká investice

1) Minimální investice

V tomto modelu půjde především o minimalizaci nákladů, z tohoto důvodu budou mít nejvyšší licence Microsoft 365 Business, která obsahuje rozšířené zabezpečení, pouze lidé, pracující s citlivými daty. Ostatní povýší pouze na licenci Office 365 Premium, kterou doposud měla jen část firmy. To alespoň částečně zlepší fungování procesů ve firmě.

V tomto modelu bude počítáno s přesunem účetního systému na Virtuální počítač s Windows. Databáze SQL DB Server Express zůstane.

Webový hosting pro minimální náklady ponecháme, v současnou chvíli není nutné pro statické webové stránky platit výkonný hosting.

Tabulka 12: Nákladový model – Minimální náklady (11) (15)

Nákladový model – Minimální náklady				
Položka	**Měrná jednotka**	**Jednotková cena**	**Počet měr. jednotek**	**Kalkulovaná cena měsíc**
Licence MS Office 365 Bus. Premium	Kč za měsíc/licence	262,50	10	2 625,00 Kč
Licence Microsoft 365 Business	Kč za měsíc/licence	422,50	3	1 690,00 Kč
Předplatné pro VM pro účetní sys. (odhad)	Kč/měsíc	500,00	1	500,00 Kč
SQL DB Server Express pro účet. sys.	Kč/měsíc	435,00	1	435,00 Kč
Hosting webové stránky	Kč/měsíc	42,00	1	42,00 Kč
Mzdové náklady na implementaci	Kč jednorázově	250,00	100	25 000,00 Kč
			Celkem za první měsíc:	30 292,00 Kč
			Celkem za další měsíce:	5 292,00 Kč
			Celkem za první rok:	88 504,00 Kč
			Celkem za další roky:	63 504,00 Kč

2) Střední investice

V tomto modelu již budeme počítat s vyššími investicemi. Licence Microsoft 365 Business dostanou všichni zaměstnanci, to zajistí velmi široké možnosti kontroly nad zařízeními, doménou a také spoustu bezpečnostních prvků.

Dále v tomto modelu budeme uvažovat nákup hardware pro zálohování, konkrétně to bude datové úložiště NAS QNAP TS-328, které nabízí 3 sloty pro disky typu SSD nebo HDD. Dále pak disková úložiště typu HDD Western Digital Red 3TB, model Red je určen přímo pro použití pro datová úložiště. Kvůli nákupu poměrně drahého hardwaru budou vyšší počáteční náklady.

Účetní systém se přesune na Virtuální počítač s Windows, na který bude přistupovat zejména účetní. Databáze zůstane stejná, jako doposud, tedy SQL DB Server Express. Tato databáze se hodí do modelu kvůli jednoduchosti při implementaci a také kvůli finanční výhodnosti.

Webový hosting se měnit nebude, protože prozatím není potřeba vyšší výpočetní výkon pro provoz webových stránek a současné řešení je finančně výhodné.

Tabulka 13: Nákladový model – Střední investice (11) (15)

Nákladový model – Střední investice				
Položka	**Měrná jednotka**	**Jednotková cena**	**Počet měr. jednotek**	**Kalkulovaná cena měsíc**
Licence Microsoft 365 Business	Kč za měsíc/licence	422,50	13	5 492,50 Kč
Předplatné pro VM pro účet. sys. (odhad)	Kč/měsíc	500,00	1	500,00 Kč
SQL DB Server Express pro účet. sys.	Kč/měsíc	435,00	1	435,00 Kč
Hosting webové stránky	Kč/měsíc	42,00	1	42,00 Kč
Mzdové náklady na implementaci	Kč/hod	250,00	100	25 000,00 Kč
Úložiště NAS QNAP TS-328	Kč jednorázově	7749,00	1	7 749,00 Kč
HDD WD Red 3TB	Kč jednorázově	2999,00	3	8 997,00 Kč
			Celkem za první měsíc:	48 215,50 Kč
			Celkem za další měsíce:	6 469,50 Kč
			Celkem za první rok:	119 379,50 Kč
			Celkem za další roky:	77 634,00 Kč

3) Velká investice

V tomto modelu můžeme věnovat prostředky na licence pro maximální zabezpečení. K licencím Microsoft 365 Business pro všechny zaměstnance, se přidají licence pro zabezpečovací modul Enterprise Mobility + Security, konkrétně licence E5. Zde jsou velice široké možnosti z pohledu procesů zabezpečení, zejména pak při použití Azure Anti Threat Protection.

Podobně jako v předchozím modelu zde budeme uvažovat nákup hardware pro zálohování, v tomto případě to bude úložiště NAS Synology DS1019+, které obsahuje 10 slotů pro HDD nebo SDD disky. Stejně jako v předchozím modelu budou použity disky typu HDD Western Digital Red 3TB

Účetní systém se přesune, stejně jako v předchozím modelu, na Virtuální počítač s Windows, na který bude přistupovat zejména účetní. Databáze zůstane stejné, jako doposud kvůli jednoduchosti při implementaci a také kvůli finanční výhodnosti.

Webový hosting se přesune pod Azure s využitím App Service. Na rozdíl od předchozího modelu zde můžeme vybrat vyšší výkon a v případě potřeby lze další výkon snadno škálovat.

Tabulka 14: Nákladový model – Velká investice (11) (15)

Nákladový model – Velká investice				
Položka	**Měrná jednotka**	**Jednotková cena**	**Počet měr. jednotek**	**Kalkulovaná cena měsíc**
Licence Microsoft 365 Business	Kč za měsíc/licence	422,50	13	5 492,50 Kč
Licence Enterprise Mobility + Security E5	Kč za měsíc/licence	212,50	3	637,50 Kč
Předplatné pro virtuální počítač pro účet. sys. (odhad)	Kč/měsíc	800,00	1	800,00 Kč
SQL DB Server Express pro účet. sys.	Kč/měsíc	435,00	1	435,00 Kč
Web hosting Azure App Service	Kč/měsíc	1242,00	1	1 242,00 Kč
Mzdové náklady na implementaci	Kč/hod	250,00	100	25 000,00 Kč
Úložiště NAS Synology DS1019+	Kč jednorázově	21090,00	1	21 090,00 Kč
HDD WD Red 3TB	Kč jednorázově	2999,00	5	14 995,00 Kč
			Celkem za první měsíc:	69 692,00 Kč
			Celkem za další měsíce:	8 607,00 Kč
			Celkem za první rok:	164 369,00 Kč
			Celkem za další roky:	103 536,00 Kč

3.2 Porovnání modelů a výběr cesty

Máme tedy na výběr ze tří investičních modelů. První model – Minimální investice je zaměřená na úsporu nákladů, ale neřeší většinu kritických míst v informačním systému firmy. Stěžejní pro většinu kritických míst je licence Microsoft 365 Business, pokud by ji měly pouze 3 lidé, kteří pracují s citlivými daty, tak by to sice částečně řešilo kritické místo *Zabezpečení citlivých dokumentů*, ale pro zbytek zaměstnanců by již dokumenty zabezpečené nebyly. Dále by v prvním modelu byla omezená správa firemního hardwaru, která je svázána s Microsoft Intune. V tomto modelu zůstane neřešené kritické místo *Zálohování dat.*

Druhý model – Střední investice již obsahuje, pro naše cíle, stěžejní licence Microsoft 365 Business pro všechny zaměstnance. Zde již kompletně překrýváme kritické místo *Zabezpečení citlivých dokumentů,* díky Azure Information Protection a *Správa a kontrola nad firemním hardwarem,* díky Microsoft *Intune*. Kritické místo Ochrana před ransomware útoky je zde částečně řešeno také. *Omezené cloudové úložiště* je zde díky Azure poměrně snadno rozšiřitelné. Oproti prvnímu modelu je zde řešeno kritické místo *Zálohování dat*. Data budou zálohována na úložiště NAS, které bude disponovat prostorem 9 TB, což umožní při současném zaplnění úložišť OneDrive a SharePoint Online držet zálohy až týdny dozadu. Softwarově se zálohy budou řešit pomocí služeb Azure vhodných pro zálohování, například Azure Backup.

Poslední model – Velká investice obsahuje na rozdíl od předchozích modelů spolu s licencemi Microsoft 365 Business, také licence Enterprise Mobility + Security pro část zaměstnanců, kteří pracují s citlivými daty. Tato licence obsahuje množství rozšíření zabezpečení, která lze využít jako ochranu proti ransomware útoky, což je jedno z kritických míst, které předchozí modely řeší jen částečně. Stejně jako u předchozího modelu zde počítáme s vyřešením kritických míst jako *Zabezpečení citlivých dokumentů, Správa a kontrola nad firemním hardwarem, Omezené cloudové.* Kritické místo *Zálohování dat,* je zde řešeno podobně jako u předchozího modelu, nákupem datového úložiště NAS. Na rozdíl od předchozího modelu je zde více kladen důraz na možnost rozšíření do budoucna, proto má vybraný model 10 slotů pro HDD nebo SDD.

Po konzultaci s manažerem firmy byl vybrán kompromisní model ***Střední náklady***, s tím, že je do budoucna možné postoupit na vyšší model, alespoň softwarově.

4 Implementace vybraných modulů MS Azure

Abych mohl provádět změny a testování v Azure ve firemní doméně, tak mi manažer přidělil některé správní role. Jako čtenář mám přístup ke všemu kromě údajů, které se týkají financí a účetnictví firmy nebo citlivých dat uživatelů. Jako editor mám přístup ke správě uživatelů, změnám v zabezpečení, správě Intune a podobně. Pokud bych potřeboval změnit nějakou zásadní věc, ke které bych neměl přístup, tak by ji změnil manažer, jako globální správce.

V zadání práce je bod – definujte optimální množinu zásad v modulu Azure Policy, zásady v tomto modulu jsou ovšem velmi obecného charakteru a souvisí hlavně s hromadnou správou velkého množství virtuálních počítačů a dalších služeb z předplatného, které by se jinak musely spravovat jednotlivě. Proto se pro zvolenou implementaci nejlépe hodí konkrétní množiny zásad týkající se přímo zvolených aplikací a služeb, jež jsou jejich přímou součástí. Vlastní zásady dodržování přepisů nabízí většina služeb jako Intune, Azure Information Protection a podobně. Zmiňované zásady budou tedy definovány konkrétně pro každou služby.

V následujících podkapitolách budou uvedeny pouze příklady využití služeb, popis plné implementace každé zmiňované služby by byl příliš dlouhý. Pro účely testování jsou využívány některé firemní počítače a mobilní telefony, plná implementace do celé firmy je sice v procesu, ale není cílem této práce.

Přístup k prostředkům, službám a aplikacím je možný přes Azure Portál, který je dostupný přes webový prohlížeč. Je také možné využít mobilní aplikaci. Další možností je přístup k některým Azure službám pomocí funkce Microsoft 365 Admin center. V Admin center je výrazně zjednodušené prostředí a ovládání služeb jako Intune, Active Directory, Azure Information Protection a podobně. Nevýhodou je ovšem méně možností v konfiguraci. Tento přístup se hodí spíše pro následnou správu, kde již budou služby implementované a nastavené.

4.1 Úprava Azure Active Directory

V Active Directory panuje ve firmě zmatek z hlediska názvů uživatelů, zařízení, členství ve skupinách a podobně. Dále zde nejsou jasně názvem odlišeny zařízení soukromá a firemní. Tato nejednotnost a zmatek může způsobit problém například při ztrátě zařízení nebo při jakékoli další manipulaci se zařízením. Nejednoznačnost pojmenování může například způsobit smazání jiného zařízení z domény a podobně.

Dále je zde rozdíl v typu připojení zařízení v Active Directory, zařízení může být buď typu AD Joined nebo AD Registred. AD Joined jsou zařízení ve vlastnictví firmy, jsou důvěryhodná. AD Registred jsou pouze přihlášená zařízení, například soukromý počítač, nebo mobilní telefon. Některá zařízení, která by měla být Joined, jsou pouze Registred. V tomto bude zaveden pořádek, tak aby firemní zařízení byla vždy Joined a šla spravovat vzdáleně.

Je třeba jasně rozlišit příslušnost zařízení, proto bude zaveden nový systém pojmenovávání. Jméno počítače bude vždy ve formátu NázevfirmyPC-Iniciály, tedy například CermitechPC-MDA. Pro telefony CermitechTEL-MDA. V případě zařízení, které bude v Active Directory jako registrované, což ve své podstatě znamená soukromý počítač nebo telefon, nelze v některých případech vynucovat název zařízení.

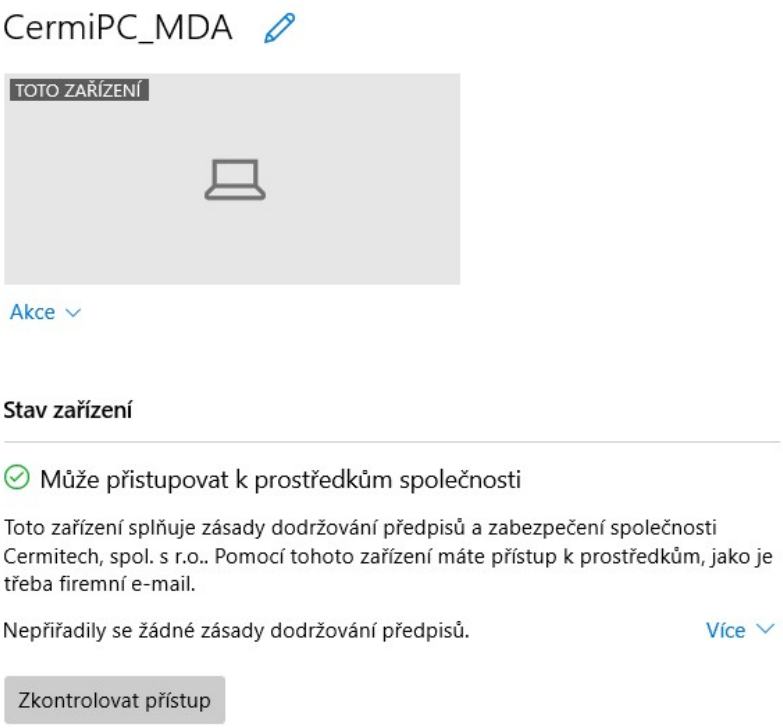
4.2 Implementace Intune

Intune je služba, která slouží ke správě mobilní zařízeních, ať už počítačů či mobilních telefonů. Integruje se spolu s dalšími službami, jako Azure Active Directory. Pomocí Intune je možné nasazovat aplikace, nastavovat Zásady dodržování předpisů a mnoho dalšího. (17)

Intune se spravuje pomocí Azure portálu, v omezené míře lze Intune spravovat také pomocí Microsoft 365 Admin center, nicméně prvotní konfiguraci je nutné provést v portálu.

Postup implementace a příklady správy na počítači s Windows:

1) Připojení počítače s Windows k Intune



Obrázek 3: Zařízení připojené k Intune

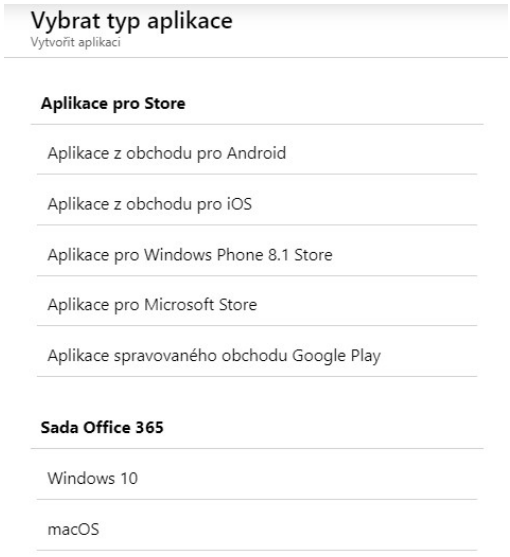
Aby bylo možné spravovat počítač s Windows pomocí Intune, je nutné nainstalovat před Windows Store aplikaci Portál společnosti. Dále je potřeba přejít ve Windows do nastavení -> Účty -> Přístup do práce nebo školy a zde připojit pracovní účet, stačí použít název firemní domény a dojde k připojení pomocí MDM a propojení s aplikací Portál společnosti. I přesto, že je počítač připojen do domény pomocí Azure Active Directory, je stále nutné připojit se jako pracovním účtem. V portálu společnosti už stačí kliknout na tlačítko připojit a vše by mělo být propojené.

V případě, že se vše propojí správně, tak se zobrazí zpráva ve Stavu zařízení, že je možné přistupovat k prostředkům společnosti.

2) Vzdálená instalace aplikací pro Windows

Z důvodu stále aktuálního softwaru, maximální efektivnosti práce a neposlední řadě také maximální využití koupeného softwaru bude v Intune definována sada aplikací, které se budou automaticky instalovat do každého firemního počítače. Tato sada bude testovací a kdykoli je možné přidat další software.

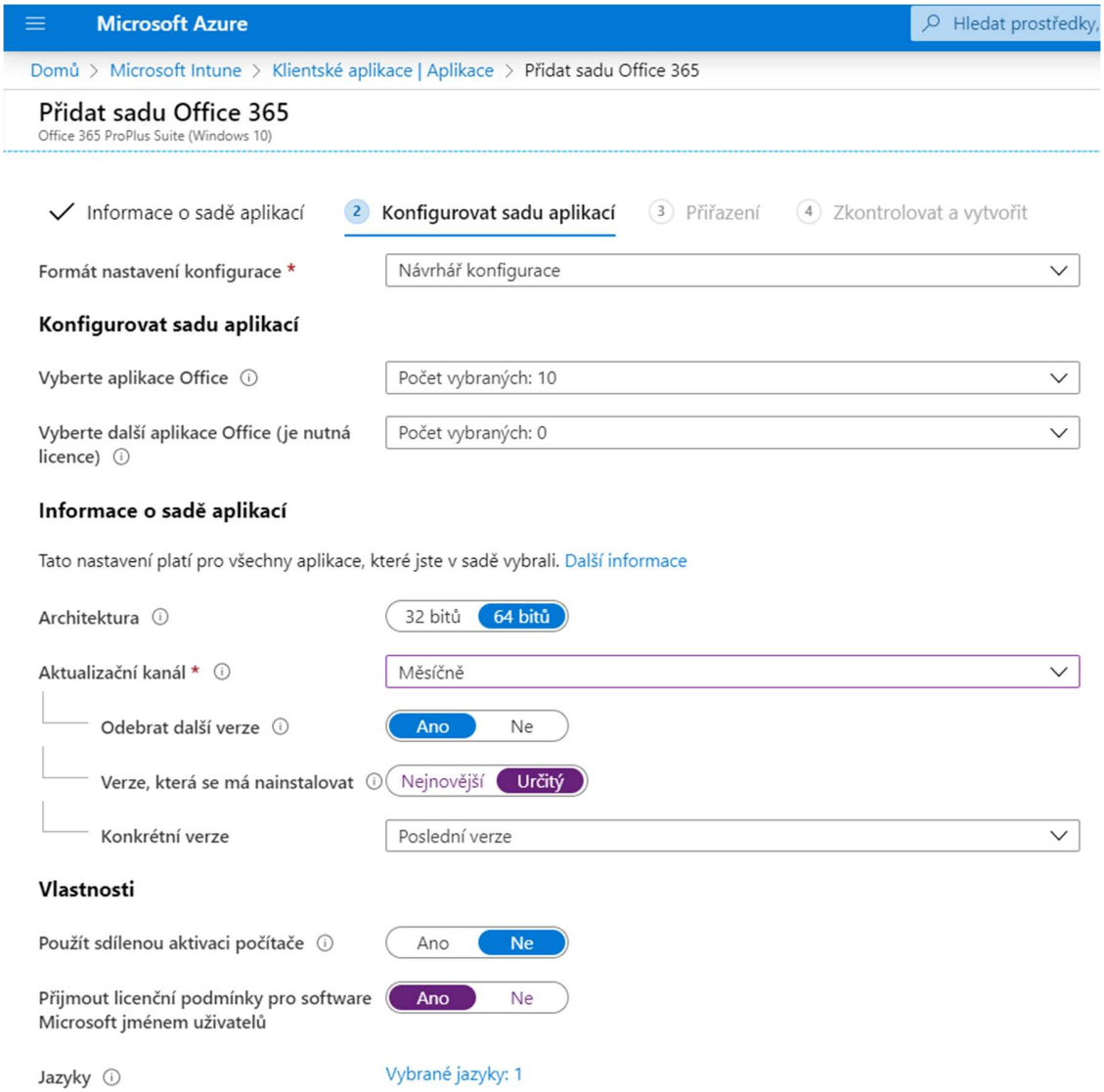
Na následujícím příkladu bude ukázáno, jakým způsobem lze přidat do klientských aplikací balík kancelářského softwaru Office a automaticky jej nainstalovat. V rozhraní pro Intune v Azure portálu se přejde na položku Klientské aplikace, následně na položku Aplikace, v horní liště je položka Přidat. Po kliknutí na tuto položku se otevře průvodce přidání aplikací, kterých je zde na výběr z velkého množství. Na obrázku níže je jen vidět menší část aplikací, ze kterých lze vybírat. Nejjednodušší je instalace aplikací z Microsoft Store nebo v případě mobilních zařízení z App Store a Google Play. Dále je možné instalovat aplikace pro Windows (Win32 s příponou .msi). Je nutné podotknout, že není možné tímto způsobem instalovat jakoukoli aplikaci. Daná aplikace musí být pro tuto instalaci přizpůsobená.



Obrázek 4: Výběr aplikací

První, co je ve většině případů na nový počítač instalováno, je sada Office 365, proto bude tato instalace uvedena jako příklad. Vybrána bude tedy položka Sada Office 365 pro Windows 10. Následně se otevře okno s prvním krokem konfigurace – Informace o sadě aplikací. Zde je standardně předdefinován název sady, popis, vydavatel a podobně. Vše je možné měnit dle potřeby. Je zde možné nastavit, jestli má být aplikace viditelná v Portálu společnosti jako vybraná aplikace.

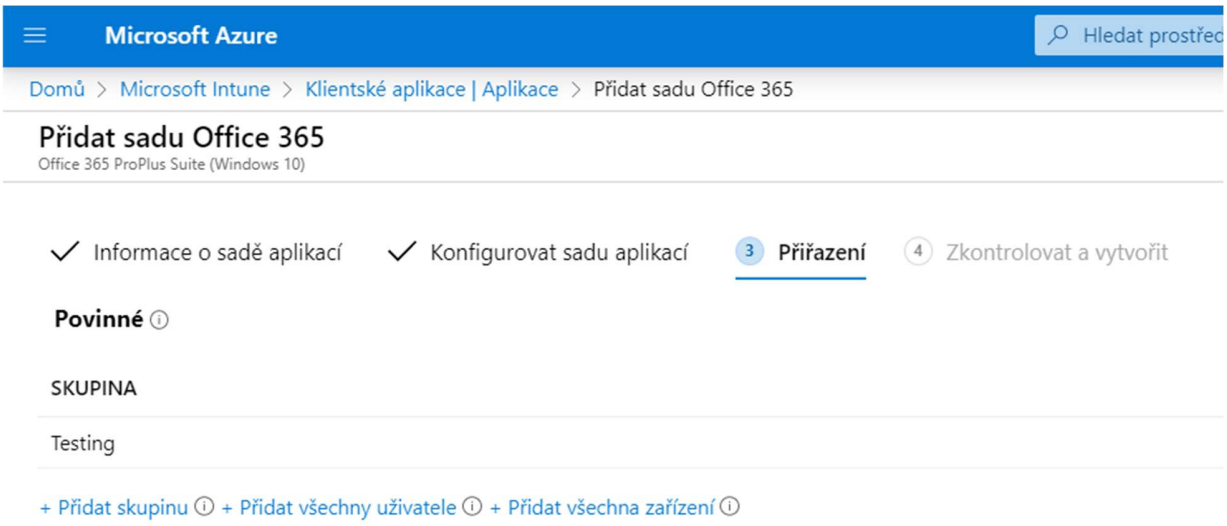
V kroku číslo 2, tedy Konfigurace sady aplikací, se přistupuje k samotnému nastavení, co má být nainstalováno, v jaké verzi a podobně. Na obrázku níže jsou tato nastavení vidět.



Obrázek 5: Konfigurace vzdálené instalace v Intune

Aby se aplikace naistalovaly automaticky na pozadí, je nutné zvolit přijmutí licenčních podmínek jménem uživatelů. Další důležitou věcí je vybrat jazykovou sadu pro dané aplikace.

Předposledním krokem je přiřazení ke skupině, uživatelům nebo zařízením. Tento systém přiřazení není využíván pouze u Intune, ale obecně na celé platformě Azure. Na následujícím obrázku je vidět přiřazení ke skupině Testing, která je vytvořená pro účel testovacího nasazení na omezeném počtu uživatelů a zařízení.



Obrázek 6: Přiřazení skupiny v instalaci v Intune

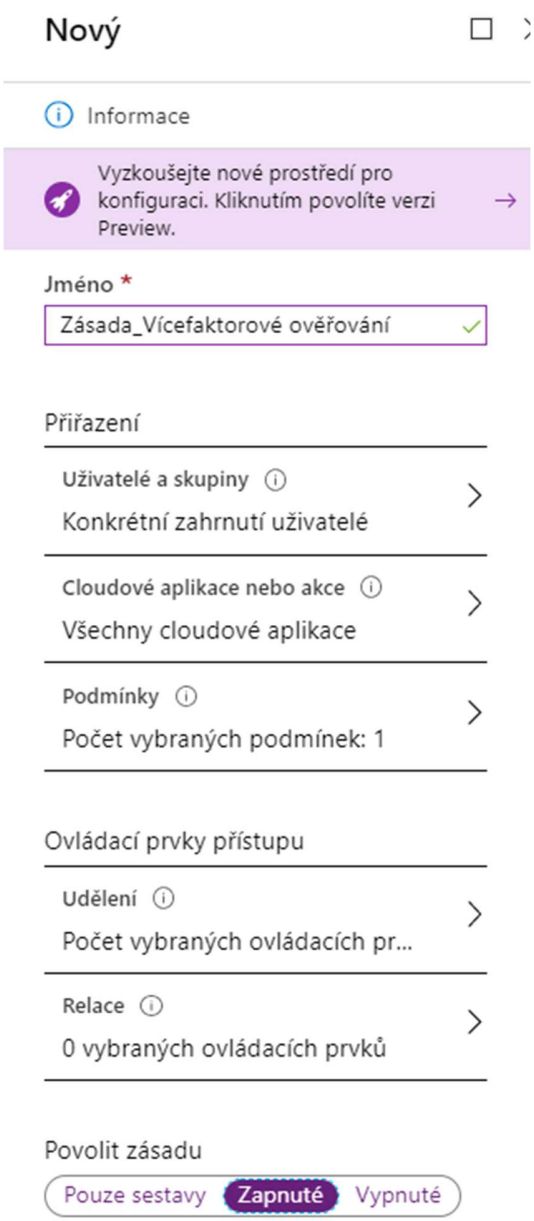
Poslední krok je pouze shrnutí instalace a konfigurace. Po potvrzení a uložení je aplikace přiřazena v seznamu instalací. Poté lze danou aplikaci přiřadit dalším uživatelům, skupinám nebo zařízením.

3) Vzdálená správa

Intune nabízí několik funkcí pro vzdálenou správu a v případě ztráty, ovládnutí nebo nějakého dalšího nepředvídatelného stavu je možné zařízení vzdáleně uzamknout. Také je zde možnost rotovat klíč BitLockeru, restartovat zařízení obnovení hesla nebo vynutit kontrolu pomocí Windows Defenderu.

4) Zásady zabezpečení

Jako jeden podrobně rozvedený příklad z mnoha lze uvést vytvoření zásady dodržování předpisů pro vícefaktorové ověřování. Častým cílem útoků bývají účty s právy správce. Tyto účtu představují při ovládnutí útočníkem obrovské riziko, toto riziko se dá minimalizovat nastavením vícefaktorového ověřování pro přihlašování.



Obrázek 7: Konfigurace zásady zabezpečení

V Intune přejdeme na položku podmíněný přístup a kliknutím na tlačítko Nové zásady se otevře panel pro konfiguraci zásad podmíněného přístupu. Na následujícím obrázku je vidět shrnutí celé konfigurace zásady. V nabídce Přiřazení -> Uživatelé a skupiny -> Role a adresáře lze vybrat, jaké role zahrnout, budou to: Globální správce, Správce SharePointu, Správce Exchange, Správce podmíněného přístupu, Správce zabezpečení, Správce helpdesku nebo správce hesel, Správce fakturace, Správce uživatele či Správce ověřování. V následující položce budou zahrnuty všechny cloudové aplikace a v podmínkách všechny platformy a prohlížeče. V nabídce Ovládací prvky přístupu a položce Udělení bude zatrhnuto *Vyžadovat vícefaktorové ověření.* Nakonec stačí už jen povolit zásadu a potvrdit celou konfiguraci. Azure ještě upozorní, že toto nastavení bude mít vliv i na právě přihlášený účet, je to proto, aby si správce omylem nezablokoval přístup. Vzhledem k povaze této zásady však můžeme zásadu uložit a aplikovat.

Další zásada, kterou bude obdobným způsobem vynucena je šifrovaní disku pomocí Bitlockeru.

Z důvodu překročení rozsahu práce není možné ukázat všechny možnosti služby Intune, proto zde byla služba v několika příkladech jen představena. Intune je postupně implementován i na zbytek firemních zařízení.

Postup implementace Intune pro mobilní zařízení

1) Připojení aplikace

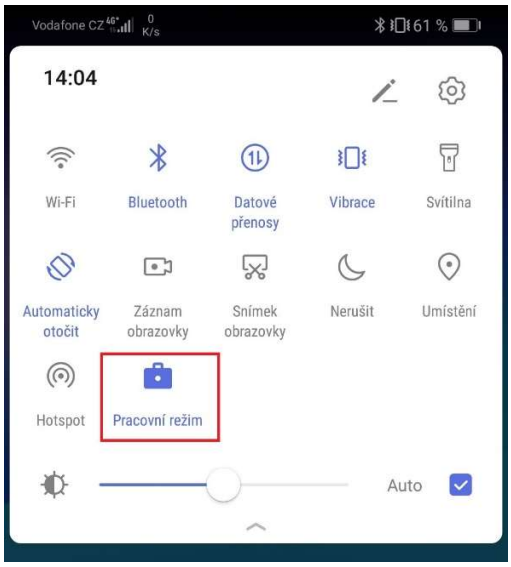
Pro správu mobilních zařízení s Androidem (je možné spravovat i zařízení Apple nebo Windows) je nutné pomocí Google Play stáhnout a nainstalovat aplikaci Intune – Portál firmy Microsoft. Aplikace po otevření slouží ve své podstatě pouze pro jednoduchou konfiguraci a připojení k Intune.

Obecně jsou zde možnosti dvě možnosti fungovaní Intune v mobilních zařízeních, a to podle rozdělení vlastnictví na:

- Osobní
- Firemní

V případě osobního vlastnictví daného zařízení, není z portálu Azure přístup k některým funkcím a také informacím o zařízení. V případě volby firemního vlastnictví je ovšem fungovaní telefonu změněno zásadně. Také v tomto případě nelze aplikaci Portál společnosti odinstalovat.

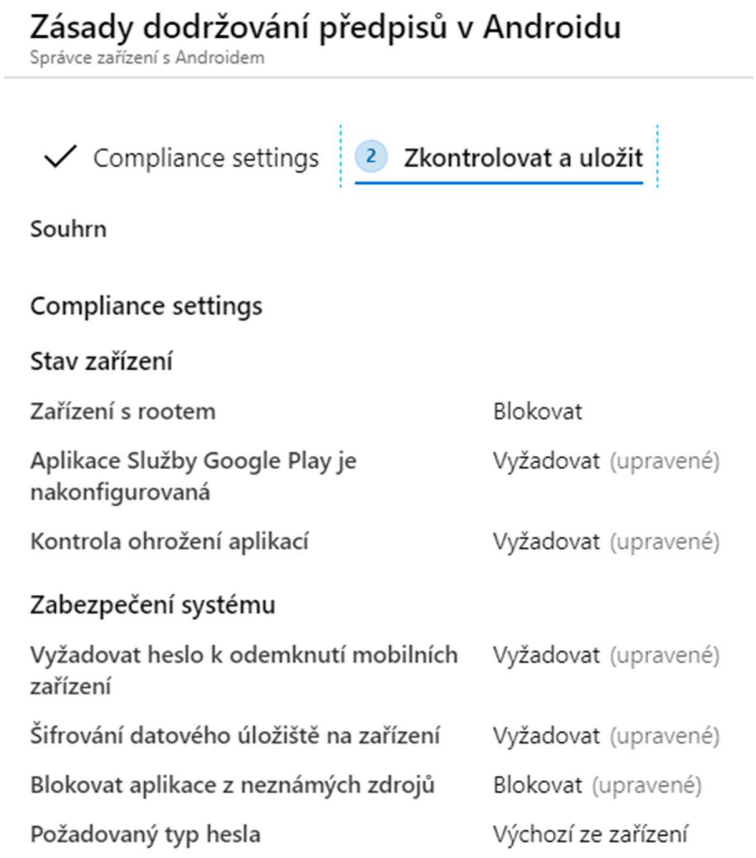
Telefon je rozdělen na dva režimy – Pracovní a Soukromý režim. Na obrázku níže je červeně označená tlačítko Pracovní režim, tímto tlačítkem se jednoduše mění režimy. V případě, že je pracovní režim vypnutý, jsou aplikace, které spadají do kategorie pracovní, zašedlé a nelze s nimi pracovat. Také se například nesynchronizují, takže v případě, že by zde byla aplikace Outlook, tak se začne synchronizovat až po zapnutí pracovního režimu.



Obrázek 8: Volba pracovního režimu v telefonu

2) Zásady dodržování předpisů

Zásady dodržování předpisů jsou u obou režimů stejné. Podstatné je například nutnost zabezpečit telefon heslem, nebo šifrování úložiště pro případ použití SD karty. Tato zásada je nastavena celé skupině uživatelů, stačí ji tedy v Azure v nastavení Intune přiřadit.



Obrázek 9: Zásady dodržovaní předpisů Android

3) Klady a zápory implementace

Po otestování aplikace a implementace v obou režimech s různým nastavením vycházejí tyto klady a zápory:

Klady:

- Vynucení zmiňovaných zásad nastavení (heslo, šifrováni…)
- Možnost oddělit profily pracovní a osobní a s tím i aplikace
- Možnost nainstalovat "jedním kliknutím" do telefonu desítky aplikací

Zápory:

- Aplikace musejí být v telefonu dvakrát, je potřeba přepínat mezi režimy, což není uživatelsky přívětivé
- Aplikace se často odhlašuje, což brání plynulému používání
- Aplikace celkově zpomaluje telefon, protože musí být neustále zapnutá na pozadí a synchronizuje se
- Zaměření firmy neumožňuje příliš často odstřihnutí se od interní komunikace (Teams chat, Outlook), takže je pracovní režim zapnutý neustále, výjimku tvoří například dovolená, tímto pracovní režim postrádá smysl
- Celkově je aplikace omezující a zpomaluje práci s telefonem

Po otestování v obou režimech s různým nastavením jsem došel k závěru, že zde zápory silně převažují nad klady a Intune v mobilních zařízeních nebude využíván. Není zde možné pouze vynutit zásady dodržování předpisů, vždy je vytvořen pracovní profil, který není vyhovující.

4.3 Azure Information Protection

Jak již bylo mnohokrát zmíněno, Azure Information Protection slouží ke klasifikaci a ochraně dat. Pro použití je nutné stáhnout si klienta, instalátor je dostupný na webu Microsoft, přes odkaz z Azure. Po nainstalování klienta se v aplikacích Office vytvoří tlačítko Citlivost, kde je možné definovat dokument podle předdefinovaných popisků. Je možné také vytvořit zásady pro automatickou klasifikaci.

Postup implementace:

1) Vygenerování popisků

V ovládacím rozhraní pro Azure Information Protection jsou pro toto konkrétní použití v zásadě důležité dvě položky, těmi jsou Popisky a Zásady. Když přejdeme na položku popisky, tak tu zatím žádný není. Je tu ovšem možné vygenerovat předdefinované popisky, které jsou vidět na obrázku níže. V zásadě by mělo pro potřeby firmy stačit rozdělení:

- Osobní
- Firemní
- Firemní citlivá

Osobní data mají svou značku, ale nebudou žádným způsobem omezena. U firemních dat je jich třeba rozlišit, zda jsou to běžné dokumenty nebo emaily, nebo se jedná například o smlouvy, nabídky, výplatní pásky a podobně. Některé popisky můžou mít podkategorie jako je tomu na obrázku níže u popisků *Citlivé* a *Vysoce důvěrné.*

Po dohodě s manažerem se nějaký čas ponechají všechny předdefinované popisky a po otestování a zavedení rutin se později může přistoupit k redukci na výše zmiňované kategorie.

Zobrazovaný název popisku	Zásady	Označení	Ochrana
Osobní	test		
Veřejná	test		
Všeobecné	test		
Citlivé	test		
Pouze příjemci	test	✓	✓
Všichni zaměstnanci	test	✓	✓
Kdokoli (nechráněný)	test	✓	
Vysoce důvěrné	test		✓
Pouze příjemci	test	✓	✓
Všichni zaměstnanci	test	✓	✓
Kdokoli(bez ochrany)	test	✓	

+ Přidat nový popisek

Obrázek 10: Popisky Azure Information Protection

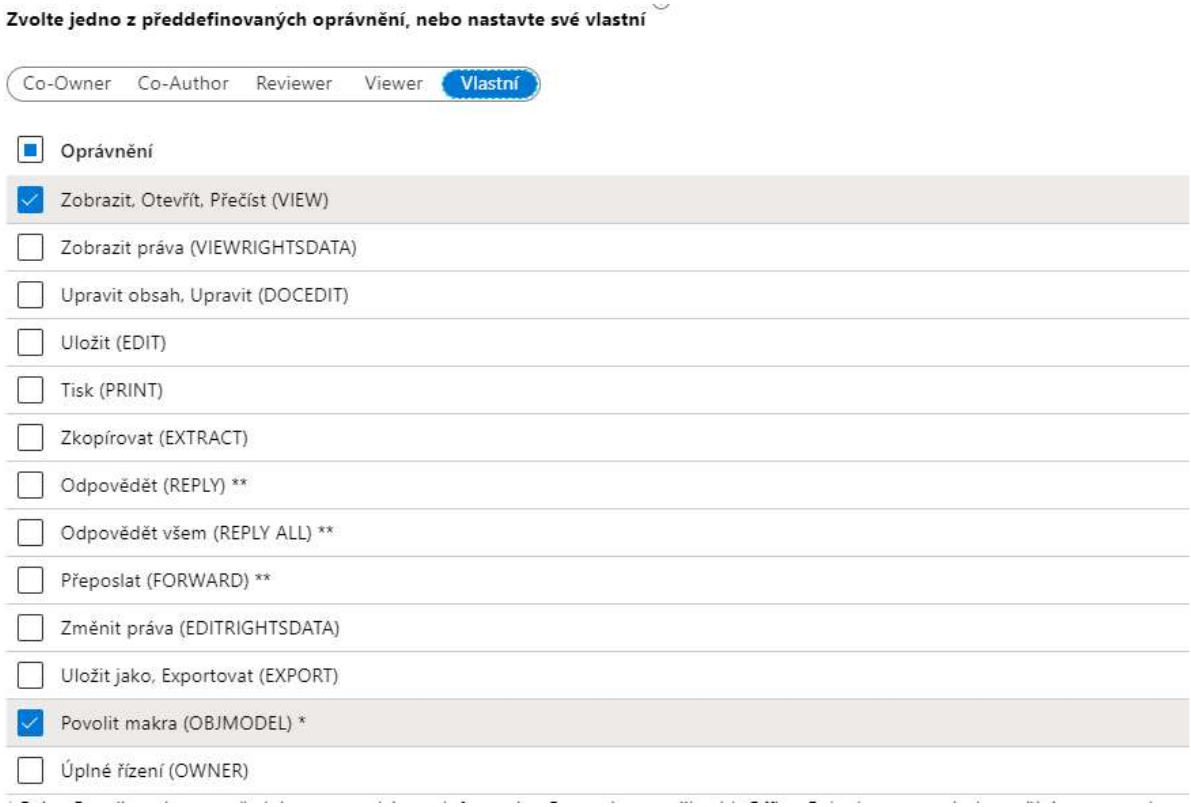
2) Konfigurace popisků

Konfigurace samotných popisků zde bude ukázána na popisku Vysoce důvěrné a obdobným způsobem budou nakonfigurovány i ostatní popisky.

Prvním krokem je povolení popisku, dále pak název a popis, který bude zobrazen u popisku pro koncové uživatele. Dále lze vybrat barvu popisku, která je zde předdefinována jako červená. Zajímavá možnost je nastavit další vizuální označení, jako je barva záhlaví, zápatí nebo vodoznak. Tyto možnosti zatím nebudou využity.

Důležitým krokem je nastavení oprávnění. U popisků, které jsou veřejné, je toto nastavení vynecháno. Jako ochrana je zde použit cloudový klíč Azure. Pro každý popisek, u kterého je vybrána ochrana cloudovým klíčem, je nutné nastavit práva pro uživatele nebo skupiny. Tento vzorový popisek bude využíván pro dokumenty, které jsou pouze pro úzké vedení firmy, proto zde bude nastaven jako spoluvlastník skupina, ve které jsou členové vedení firmy. Tímto způsobem je zajištěno, že pokud by se citlivý dokument s popiskem Vysoce důvěrné dostal k někomu jinému než k uživateli z této skupiny, tak k němu neautorizovaný uživatel nebude mít přístup. Na následujícím obrázku jsou ukázány možnosti dalšího vlastního nastavení přístupu a práv. Mimo již zmiňovaný zákaz přeposílání, lze zakázat například tisk, uložení, export a tak dále. V tomto popisku bude mít spoluautor (Co-Author) všechna práva kromě změny práv a exportu. Čtenář (Viewer) bude mít povoleno pouze zobrazení a čtení.

Hodí se podotknout, že oprávnění pro popisek lze přidat i pro externí uživatele pomocí emailové adresy, nebo dokonce pro celou doménu (@externifirma.cz).



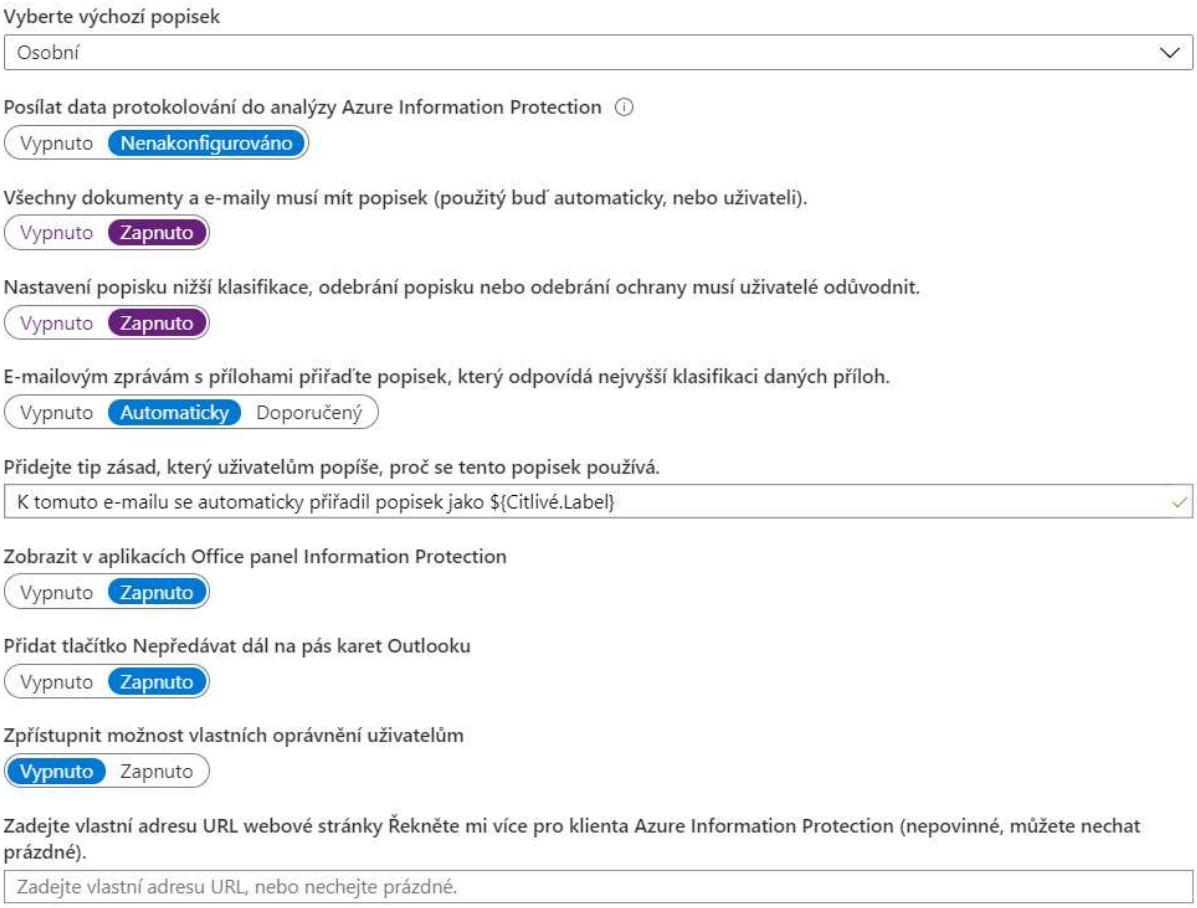
Obrázek 11: Oprávnění u popisků

Velmi zajímavou možností je také konfigurace podmínek pro automatické použití daného popisku. Jednou ze stovek možností, je vyhledávání čísel kreditních karet v dokumentech. Pokud bude tato možnost vybrána, všechny dokumenty, ve kterým bude nalezeno standardní číslo kreditní karty, budou označeny automaticky daným popiskem s nastavenou ochranou. Další možnosti z finančního sektoru je vyhledávání čísla IBAN (mezinárodní číslo bankovního účtu). Kromě těchto předdefinovaných možností, je možné také vytvořit vlastní zásadu, kde se bude vyhledávat konkrétní textový řetězec, nebo dokonce regulární výraz.

3) Nastavení zásad

Tyto popisky jsou zatím standardně nakonfigurované. Pro aplikování popisků je nutné přejít na položku *Zásady*, kde je možné definovat zásady používání popisků. Jako první je nutné definovat název a popis zásady, dále pak vybrat uživatele či skupinu, pro které má daná zásada platit, tito uživatelé musejí mít povolený email. Dalším krokem ve vytvoření zásady je přidání popisků, které mají pro danou skupinu nebo uživatele platit.

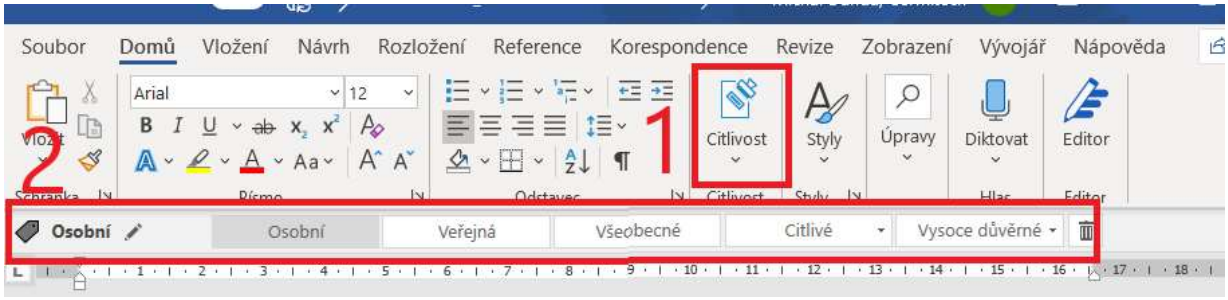
Druhá část konfigurace zásad je ukázána na obrázku níže. Podstatný je zde výběr výchozího popisku, který bude u každého dokumentu nebo emailu. Pro testovací účely bude výchozí popisek Osobní, je ale možné, že se po otestování změní na Všeobecný. Toto rozhodnutí ovšem náleží manažerovi firmy. V této zásadě je dále nastaveno, že všechny dokumenty či emaily musí mít povinně popisek, dále že při nastavení popisku s nižší klasifikací, musí být tato změna uživatelem odůvodněna. Emailovým zprávám s přílohou bude nastaven popisek s nejvyšší klasifikací dané přílohy. Dále jsou zde už jen nastavení zobrazení tlačítek v panelech, které jsou standardně vidět a jako poslední je zakázáno nastavení vlastních oprávnění uživatelů. Toto bude obecná zásada, která bude testována v chodu firmy.



Obrázek 12: Konfigurace zásad AIP

4) Praktické používání

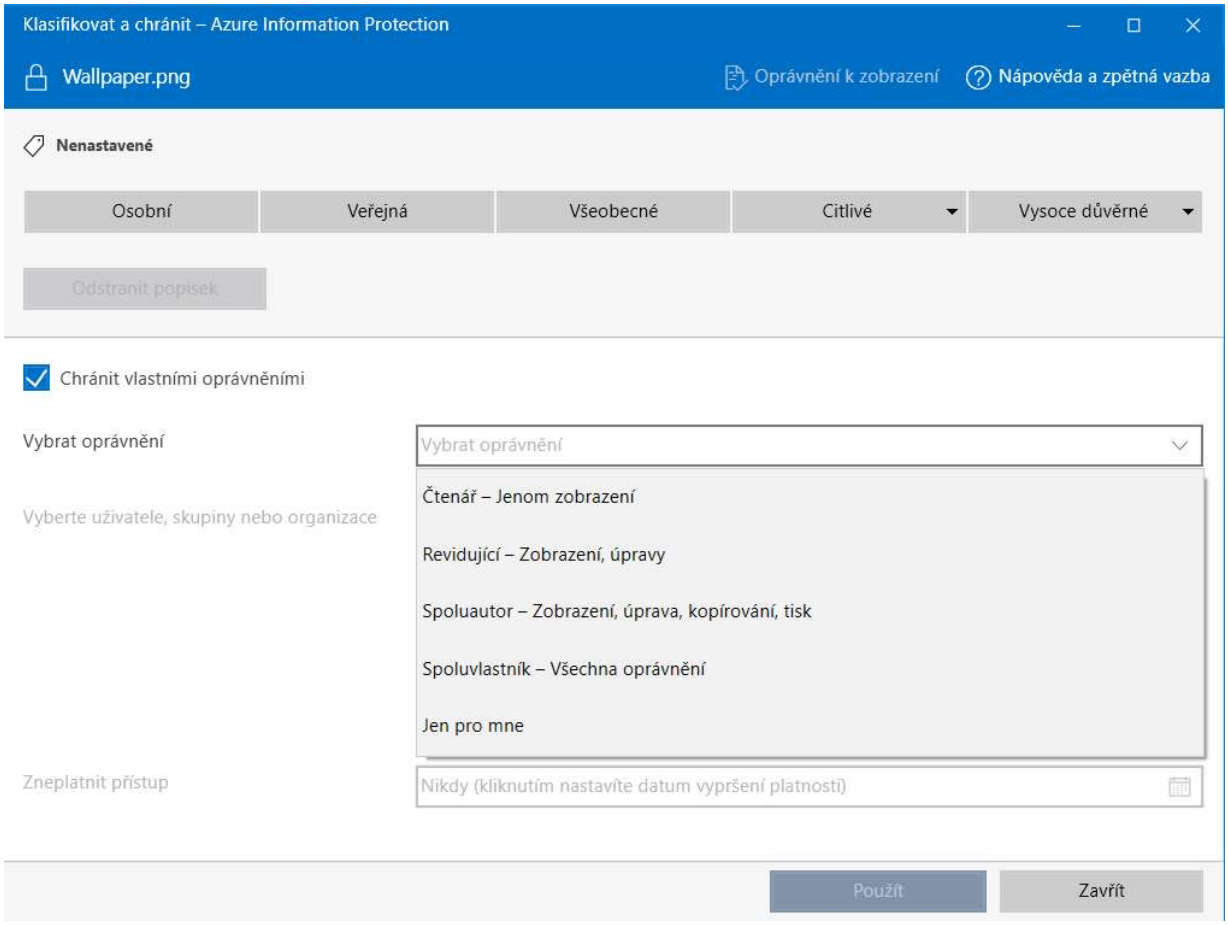
Příklad klasifikace dat bude uveden na dokumentu Microsoft Word. Na následujícím obrázku je vidět v pásu karet položka Citlivost (označeno 1), po kliknutí vyjede pás položek označený číslem 2. Zde je již možné manuálně klasifikovat dokument podle potřeby.



Obrázek 13: Panel AIP v MS Word

Podobně jako je tomu u dokumentů, je to i u emailů. V případě nového emailu je nutné zadat, stejně jako u příkladu s MS Word, citlivost dokumentu. V případě nastavení *Pouze příjemci*, není možné příchozí email kopírovat, tisknout nebo přeposílat. V případě nastavení citlivosti *Všichni zaměstnanci*, mají právo na zobrazení a úpravy pouze zaměstnanci.

Kromě klasifikace a ochrany, která je integrovaná přímo v aplikacích Office, umožňuje Azure Information Protection chránit a klasifikovat většinu dalších souborů a dokumentů mimo Office. K tomu se využívá přímo klient Azure Information Protection. Pokud bych chtěl chránit přístup například pro obrázek ve formátu .png, tak kliknu pravým tlačítkem myši na ikonu obrázku a z nabídky vyberu *Klasifikovat a chránit.* Následně se otevře zmiňovaný klient, kde je možné, podobně jako v aplikacích, vybrat popisek. Další možností je vlastní nastavení práv, což je vidět na obrázku níže.



Obrázek 14: Klasifikace AIP

5) Výhody a nevýhody daného řešení

V této kapitole byl uveden postup implementace Azure Information Protection na několika příkladech, není možné popsat celou implementaci, protože by to přesáhlo rozsah této práce. Tato testovací implementace je prozatím přidělena jen pro několik vybraných zaměstnanců a je velmi pravděpodobné, že po vyzkoušení dojde k zjednodušení a zmenšení počtu popisků. Dále bude nutné vybrat ideální výchozí popisek a definovat další standardní textové řetězce pro automatickou klasifikaci dat, tímto bude podstatně zjednodušena práce.

4.4 Zálohování dat na NAS

Původně zamýšlené řešení zálohování dat Office 365, což zahrnuje Exchange server, SharePoint Online, OneDrive pro firmy a Teams data, s využitím Azure není možné. Po bližším prozkoumání služeb a možností Azure z hlediska zálohování bylo zjištěno, že Azure žádnou takovou možnost neposkytuje. Služby jako Azure Backup slouží pouze pro zálohování na cloudová úložiště Azure, nikoli na lokální úložiště.

Pro tyto účely existuje několik služeb externích poskytovatelů (mimo Microsoft). Jedním z nich je Veeam Backup. Pro zálohování bude tedy využito této služby, nicméně to nebude popsáno v této práci, protože to nesouvisí s Azure a tím to není relevantní pro tuto práci. Veeam funguje jako samostatná služba se svým klientem.

4.5 Implementace účetního systému s využitím Azure

Jak již bylo zmiňováno v předchozích kapitolách, účetní systém bude fungovat na virtuálním počítači. Vzhledem k tomu, že zaměstnanci firmy, kteří potřebují přístup do účetnictví, budou mít nainstalovaný systém přímo ve svém počítači, tak bude virtuální počítač využíván hlavně externí účetní. Tento fakt dovoluje toto řešení, protože v případě, kdy by byl větší počet lidí, kteří by virtuální počítač využívali, tak by se navzájem mohli omezovat v přístupu.

V této kapitole půjde především o vytvoření virtuálního počítače a jeho následnou konfiguraci. Samotná instalace databáze či účetního systému již není předmětem této práce.

Postup vytvoření VM:

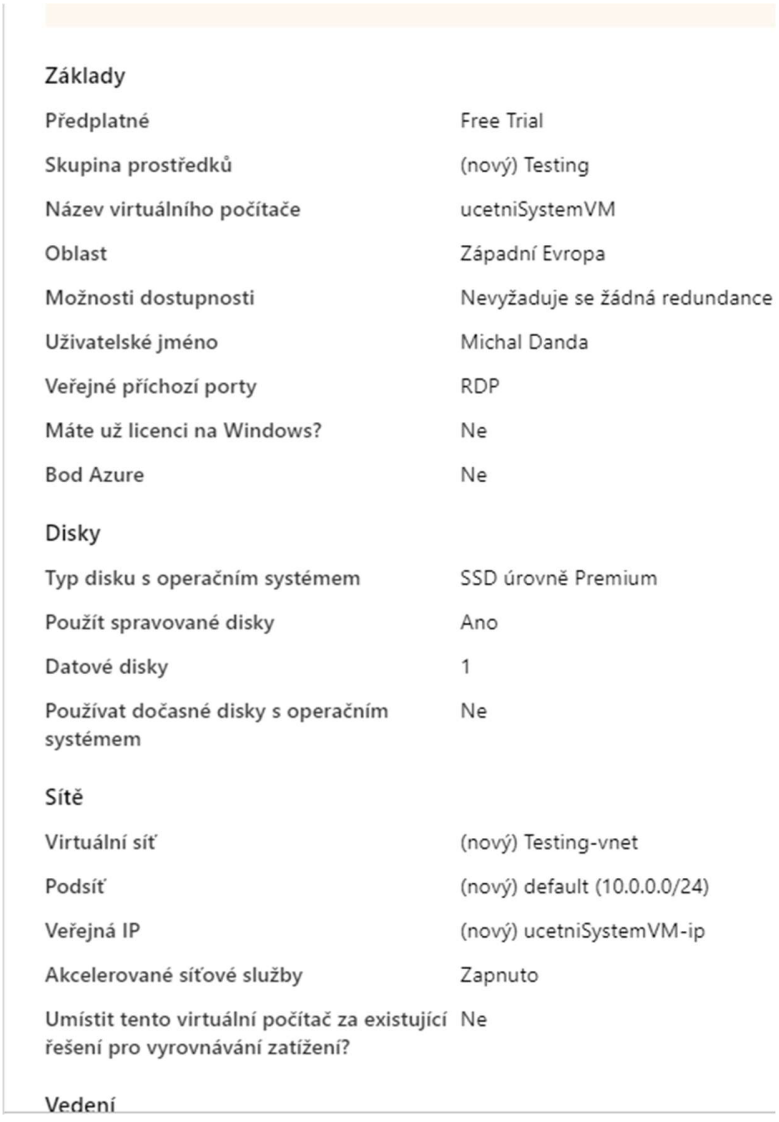
1) Vytvoření prostředku v Azure

Prvním krokem je vytvoření prostředku v Azure portálu, dále zvolení položky Virtuální počítače a následně kliknout na položku Přidat, která otevře menu pro konfiguraci VM. Nejprve je nutné nastavit předplatné, z kterého se budou odečítat platby podle využití VM. Pro účely testování nabízí Microsoft testovací účet s kreditem 170€, který pro tyto účely zdaleka stačí. Jako předplatné vybereme Free Trial. Po uplynutí doby 30 dnů bude nutné předplatit si tyto služby reálně. Dále je již nastavení VM, kde se volí jméno počítače – ucetniSystemVM, oblast – Západní Evropa, a za další operační systém virtuálního počítače. Zde je možné vybrat z několika distribucí Linuxu (SUSE, CentOS, Debian, Ubuntu), dále pak i z verzí Windows, kde je na výběr mezi Servery a klasickou verzi Windows 10 Pro. Zde zvolíme Windows 10 Pro. Další podstatnou věcí je výběr výpočetního výkonu, což bylo zmiňováno v kapitole zabývající se licencemi. Zde vybereme verzi *Standard D2s v3 (2 vcpu, 8 GiB paměti),* která by měla postačit pro potřeby účetního systému. V případě nedostatku výkonu lze poměrně snadno sestavu změnit. Následně je nutné zvolit jméno a heslo pro správce počítače.

Podstatnou částí konfigurace je také nastavení pro příchozí spojení, které bude používat protokol RDP (remote desktop protokol). Pro počáteční fázi testování, které bude probíhat paralelně s již zaběhnutým hostování účetního systému přes iPodnik, bude mít počítač veřejnou IP adresu, takže připojení nebude tak bezpečné. Nicméně po fázi testování bude použit přístup přes VPN službu Azure, což zajistí vyšší míru zabezpečení, nicméně v této fázi nemá smysl něco takového zavádět, protože by to zabralo příliš mnoho času.

V záložce Disky je možné vybrat mezi HDD a SSD disky úrovně premium a standard, vzhledem k minimálnímu rozdílu v ceně zde zvolíme SSD premium.

Dále na záložce sítě můžeme konfigurovat virtuální síť, podsíť, porty a podobně. Zde prozatím ponecháme výchozí nastavené, které vytvoří virtuální síť a veřejnou adresu. Zbytek dalších pokročilých nastavení ponecháme ve výchozím stavu. Na následujícím obrázku můžeme vidět shrnutí nastavení VM. Nyní již stačí zvolit tlačítko vytvořit a o pár desítek sekund později bude virtuální počítač připravený.



Základy

Předplatné	Free Trial
Skupina prostředků	(nový) Testing
Název virtuálního počítače	ucetniSystemVM
Oblast	Západní Evropa
Možnosti dostupnosti	Nevyžaduje se žádná redundance
Uživatelské jméno	Michal Danda
Veřejné příchozí porty	RDP
Máte už licenci na Windows?	Ne
Bod Azure	Ne

Disky

Typ disku s operačním systémem	SSD úrovně Premium
Použít spravované disky	Ano
Datové disky	1
Používat dočasné disky s operačním systémem	Ne

Sítě

Virtuální síť	(nový) Testing-vnet
Podsíť	(nový) default (10.0.0.0/24)
Veřejná IP	(nový) ucetniSystemVM-ip
Akcelerované síťové služby	Zapnuto
Umístit tento virtuální počítač za existující řešení pro vyrovnávání zatížení?	Ne

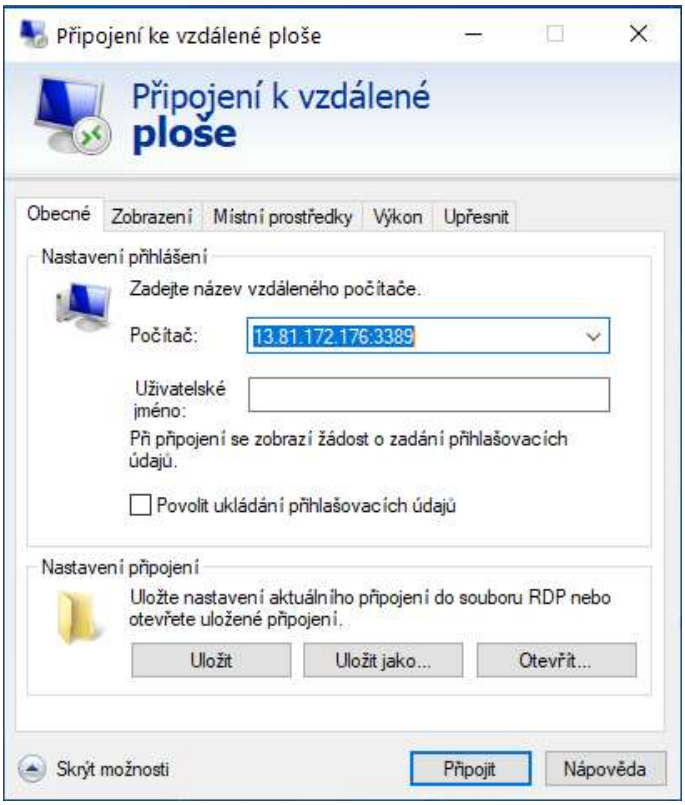
Vedení

Obrázek 15: Nastavení VM

2) První spuštění VM

Před připojením na virtuální počítač je nutné přejít v rozhraní pro VM na položku Spustit příkaz. Zde je možné spustit powershell scripty pro VM, dokonce jsou tu již některé skripty předdefinované. Z těchto skriptů spustíme *EnableAdminAccount,* který dovolí přihlášení na VM pomocí účtu správce a další *DisableNLA,* který zakáže autentizaci pomocí domény, což je pro tyto účely nutné, jinak by se nešlo vzdáleně připojit pomocí RDP z počítače, který není připojený ve stejné doméně jako daný VM. Aby se změny projevily, je nutné virtuální počítač restartovat. Když přejdeme v rozhraní na položku přehled, tak je zde možné VM na liště restartovat. Poté budou již změny zapsané.

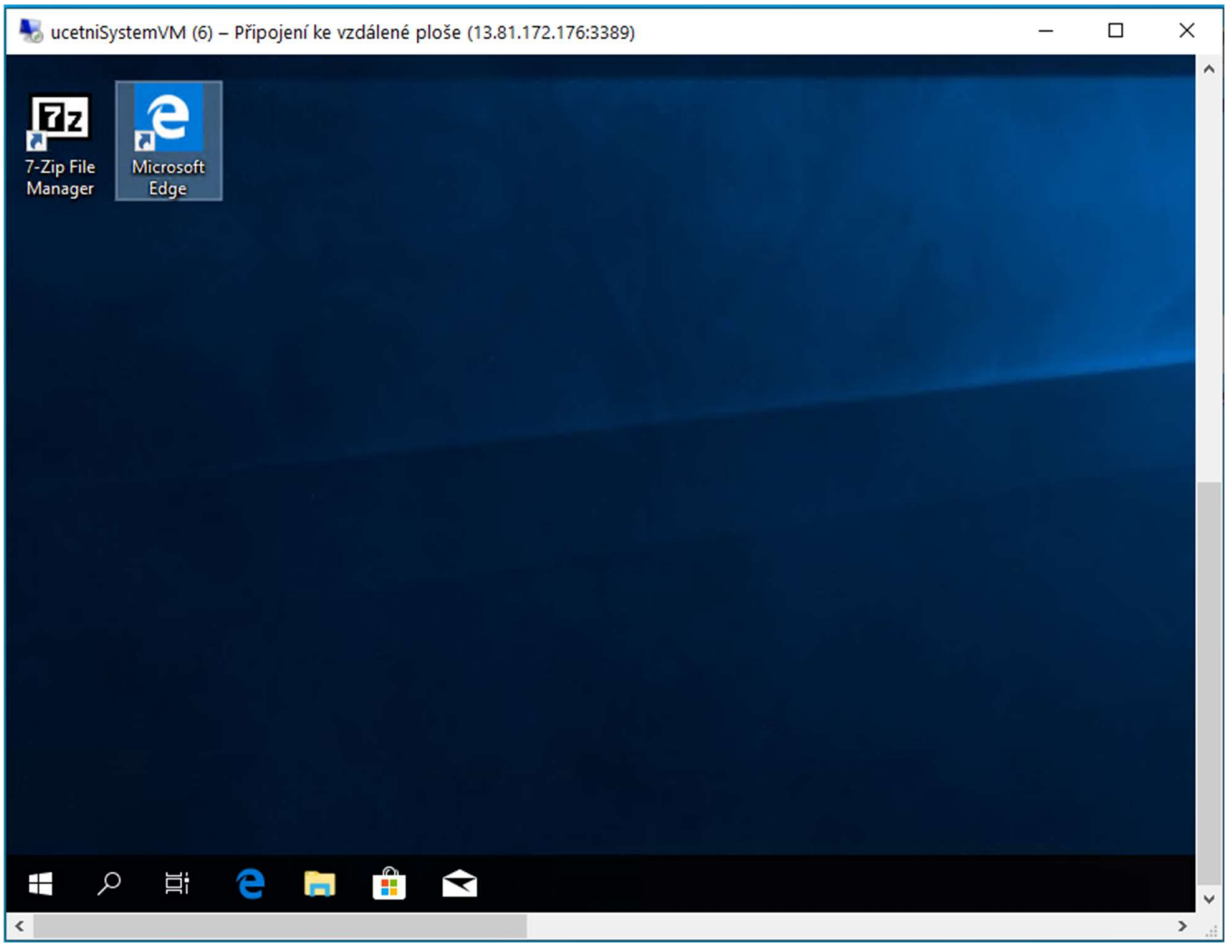
Nyní na tomto panelu klikneme na Připojit, vybereme RDP a následně klineme na stáhnout soubor. Stáhne se konfigurační soubor s příponou .rdp, který spustí integrovaného klienta pro připojení ke vzdálené ploše.



Obrázek 16: Připojení RDP

3) Fungování virtuálního počítače

Po připojení a přihlášení se, se dostaneme na plochu virtuálního počítače, kterou je možné vidět na následujícím obrázku. Nyní již stačí nainstalovat Microsoft SQL Server, účetní systém, z důvodu synchronizace také OneDrive a nakonfigurovat účet Windows pro přístup dalších uživatelů. Počítač nyní běží paralelně se stávajícím systémem přístupu k účetnictví a poté, co bude schválena finální konfigurace, se může přejít z trial verze, na placenou verzi a tím zrušit původní systém přístupu k účetnictví.



Obrázek 17: Plocha virtuálního počítače

Závěr

Tato bakalářská práce měla několik základních cílů. Prvním z nich bylo seznámit se s relevantními aplikacemi, službami, obecně s Microsoft Office 365 a zejména s Microsoft Azure. Zde jsem vybral a popsal pouze několik služeb a modulů týkajících se zabezpečení a řízení procesů, jelikož je tato platforma nesmírně rozsáhlá a nelze zde zmínit vše. V práci jsem se věnoval i licenční politice platformy Azure, neboť hraje v rozhodovacích procesech jeho implementace důležitou roli a přímo závisí na financování předpokládaného záměru.

Ve druhé části jsem se již zaměřil na praktickou analýzu informačního systému firmy, fungování procesů, používaného softwaru, služeb a podobně. Z analýzy vyplynulo, že ve firmě panují nedostatky, a to zejména v licencích, které chybějí pro část zaměstnanců. Tyto nedostatky ovšem nejlépe vystihují vytyčená kritická místa informačního systému a následný obecný návrh teoretických možností.

Ve třetí části jsem navrhl tři nákladové modely, které se liší především cenou, vybranými licencemi, službami a případně i hardwarem. Každý model nabízí jistá možná řešení. Po konzultaci s manažerem firmy byl vybrán kompromisní model Střední náklady. Poznatků a zkušeností nabytých v rámci této bakalářské práce zadávající firma skutečně využila a na základě výsledků nakoupila licence pro všechny zaměstnance podle modelu Středních investic.

V poslední části se věnuji implementaci vybraných služeb vycházejících z předchozích analýz. Tyto služby jsem aplikoval na testovací účty a počítače ve firmě. Z důvodu velké rozsáhlosti služeb, které jsem implementoval, jsou postupy realizace popsány vždy na části dané služby, nikoli na celé implementaci. U každé použité služby jsou definovány určité zásady dodržování přepisů (Policies), které souvisí se zabezpečením. Dané využití Azure pokrývá většinu definovaných kritických bodů. Zabezpečení citlivých dokumentů je řešeno pomocí AIP. Správu a kontrolu nad firemním hardwarem pomocí služby Intune, která si vynucuje určité zásady, naopak není výhodné aplikovat na mobilních zařízeních. Částečně se pro informační systém stává také kritickým bodem Konfigurace nového hardwaru, kam je možné vzdáleně nainstalovat některé aplikace pomocí služby Intune. Nejednotnost v Active Directory byla vyřešena zavedením zásad pro pojmenování a zařazení. Kritický bod, který nelze

splnit v rámci zadání práce, je zálohování dat na NAS, protože v průběhu práce bylo zjištěno, že Azure neposkytuje potřebné funkce k externímu zálohování, a proto bude nutné tento bod řešit externím softwarem. Posledním kritickým místem je účetní systém. Tento podstatný bod byl vyřešen zavedením virtuálního počítače, na kterém běží účetní software, který je na rozdíl od předchozího řešení možné plně spravovat a přistupovat k němu odkudkoli.

Každá zmiňovaná služba, jako Intune, AIP nebo Virtuální počítač, má extrémně širokou paletu možností, které lze konfigurovat a implementovat. V této práci nebyl prostor pro zabíhání do přílišných detailů, proto bylo možné zmínit jenom zlomek z věcí, které tyto služby nabízejí. Při konfiguraci a implementaci již zmíněných služeb, jsem narazil na další desítky potencionálních možností pro zlepšení běhu firmu, které bych doporučil k dalšímu prozkoumání.

Citovaná literatura

1. **HARVEY, Cynthia.** What is Microsoft Azure? *Datamation* . [Online] Datamation, 27. Květen 2017. [Citace: 1. Květen 2020.] https://www.datamation.com/cloud-computing/microsoft-azure.html.

2. **Microsoft.** Co je cloud computing? *Microsoft Learn.* [Online] Microsoft, 14. Květen 2020. [Citace: 14. Květen 2020.] https://docs.microsoft.com/cs-cz/learn/modules/principles-cloud-computing/2-what-is-cloud-computing.

3. **Wade, Matt.** An everyday guide to Microsoft Office 365 Groups. *jumpto365.* [Online] jumpto365, Inc., 3. Květen 2020. [Citace: 10. Květen 2020.] http://icansharepoint.com/everyday-guide-office-365-groups/.

4. **Jacobsen, Lola.** Microsoft Teams. *Docs Microsoft.* [Online] Microsoft, 1. Leden 2019. [Citace: 11. Březen 2020.] https://docs.microsoft.com/en-us/microsoftteams/teams-overview.

5. **Shumate, Kaarin.** Introduction to SharePoint Online. *Docs Microsoft.* [Online] 29. Červen 2018. [Citace: 16. Březen 2020.] https://docs.microsoft.com/en-us/sharepoint/introduction.

6. **Microsoft.** Co je SharePoint? [Online] Microsoft, 2019. [Citace: 10. Leden 2020.] https://support.office.com/cs-cz/article/co-je-sharepoint-97b915e6-651b-43b2-827d-fb25777f446f.

7. —. Microsoft Enterprise Mobility + Security. *Microsoft.* [Online] Microsoft, 2020. [Citace: 20. Březen 2020.] https://www.microsoft.com/en-us/microsoft-365/enterprise-mobility-security.

8. —. Management and governance. *Microsoft Azure.* [Online] Microsoft, 2020. [Citace: 15. Leden 2020.] https://azure.microsoft.com/en-gb/product-categories/management-tools/.

9. —. Identity and access management (IAM). *Microsoft Azure.* [Online] Microsoft, 2020. [Citace: 15. Leden 2020.] https://azure.microsoft.com/en-gb/product-categories/identity/.

10. —. Security. *Microsoft Azure.* [Online] Microsoft, 2020. [Citace: 16. Leden 2020.] https://azure.microsoft.com/en-gb/product-categories/security/.

11. —. Microsoft 365 pro firmy. *Microsoft 365.* [Online] Microsoft, 2020. [Citace: 20. Únor 2020.] https://www.microsoft.com/cs-cz/microsoft-365/business#office-ProductsCompare-ipaq01s.

12. —. Transformujte svůj podnik s Microsoftem 365. *Microsoft 365.* [Online] Microsoft, 2020. [Citace: 26. Březen 2020.] https://www.microsoft.com/cs-cz/microsoft-365/compare-microsoft-365-enterprise-plans.

13. —. Ceny za Azure Active Directory. *Microsoft Azure.* [Online] Microsoft, 2020. [Citace: 20. Březen 2020.] https://azure.microsoft.com/cs-cz/pricing/details/active-directory/.

14. —. Ceny řešení Enterprise Mobility + Security. *Microsoft.* [Online] Microsoft, 2020. [Citace: 6. Březen 2020.] https://www.microsoft.com/cs-cz/microsoft-365/enterprise-mobility-security/compare-plans-and-pricing.

15. —. Ceny Windows Virtual Machines. *Microsoft Azure.* [Online] Microsoft, 2020. [Citace: 5. Duben 2020.] https://azure.microsoft.com/cs-cz/pricing/details/virtual-machines/windows/.

16. —. Azure SQL Database. *Microsoft Azure.* [Online] Microsoft, 2020. [Citace: 14. Březen 2020.] https://azure.microsoft.com/cs-cz/services/sql-database/.

17. —. Microsoft Intune is an MDM and MAM provider for your devices. *Microsoft Docs.* [Online] Microsoft, 14. Říjen 2019. [Citace: 28. Duben 2020.] https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune.

18. —. Limity, kvóty a omezení předplatného a služeb Azure. *Microsoft Azure.* [Online] Microsoft, 21. Duben 2020. [Citace: 28. Duben 2020.] https://docs.microsoft.com/cs-cz/azure/azure-resource-manager/management/azure-subscription-service-limits?toc=/azure/guides/developer/toc.json.