Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Návrh a realizace migrace infrastruktury na Microsoft Azure

Diplomová práce

Autor práce: Bc. LEOŠ KARÁSEK
Studijní obor: Aplikovaná Informatika

Vedoucí práce: doc. Mgr. JOSEF HORÁLEK, Ph.D.

Hradec Králové 2023

Prohlášení

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury

.....

Leoš Karásek

10. srpna 2023

Poděkování

Děkuji vedoucímu diplomové práce doc. Mgr. Josefu Horálkovi, Ph.D. za metodické vedení práce, věcné připomínky, dobré rady a vstřícnost, při konzultacích a vypracování diplomové práce.

Anotace

KARÁSEK, Leoš. Návrh a realizace migrace infrastruktury na Microsoft Azure. Hradec Králové: Fakulta informatiky a managementu Univerzity Hradec Králové, 2023. 39 s. Diplomová práce.

Cílem této práce je posouzení možností, nákladů a možných procesů pro přechod počítačové infrastruktury z řešení on premise do Azure, cloudu společnosti Microsoft.

Cloudové technologie udělaly za posledních pár let hodně velké pokroky. Dnes se se dá říci, že se jedna o služby, které jsou stabilní, výkonné, dobře konfigurovatelné a monitorované.

Organizace čím dál více uvažují, nebo rovnou přecházejí na cloudové služby. Některé přesouvají celou infrastrukturu do cloudového řešení se všemi výhodami či nevýhodami, některé volí hybridní řešení.

Hlavní přínos práce spočívá v prozkoumání možností, výhod a nevýhod migrace do cloudové infrastruktury a umožnit podnikům takovéto zásadní rozhodnutí učinit.

Budu postupovat rešerší a následnou analýzou možností a vlastností cloudu versus on prem řešení.

Anotation

Title: Design and implementation of infrastructure migration to Microsoft Azure

The aim of this thesis is to assess the options, costs and possible processes for migrating computer infrastructure from an on premise solution to Azure, Microsoft's cloud,

Cloud technologies have made a lot of great advances in the last few years. Today, it can be said that these are services that are stable, powerful, well configured and monitored.

Organisations are increasingly considering or moving straight to cloud services. Some are moving their entire infrastructure to a cloud solution with all the advantages or disadvantages, some are opting for hybrid solutions.

The main contribution of this paper is to explore the possibilities, advantages and disadvantages of migrating to cloud infrastructure and to enable enterprises to make such a crucial decision.

I will proceed by researching and then analyzing the options and features of cloud versus on prem solutions.

Obsah

Seznam obrázků

Seznam tabulek

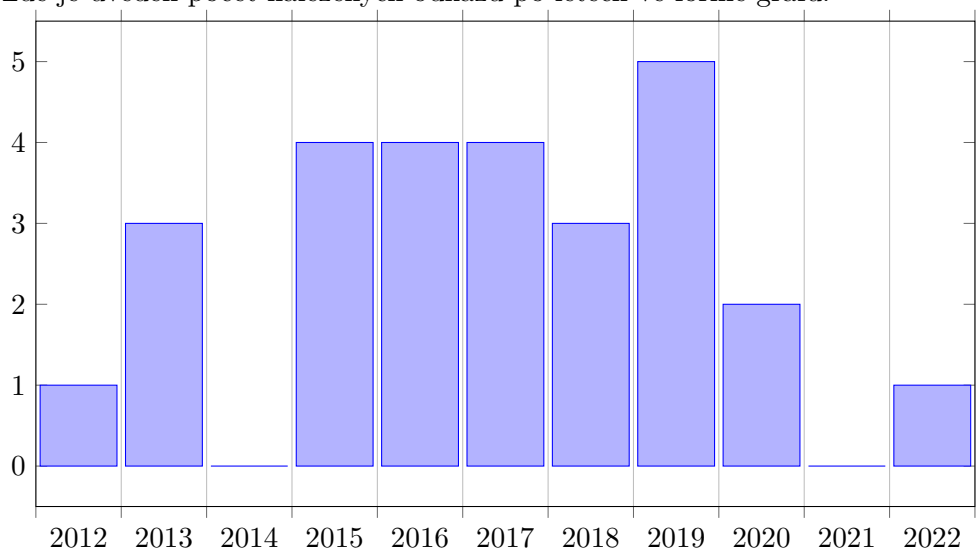
1 Úvod

"V současné době je možné, aby organizace platily pouze za to, co využívají, tedy za výpočetní výkon, úložiště, kapacitu, nebo energie. To umožňuje snížit organizacím investice do Information technologies - Informační technologie (IT), protože nemusí investovat do datových center dimenzovaných na maximální kapacitu, tedy takovou, kterou odhaduji, že budou někdy možná potřebovat. To vede k efektivnějšímu využívání sdílených datových center a umožňuje organizacím si služby IT, které potřebují najmout, a získat tím tu výhodnou možnost, že pronajaté služby mohou pružně růst nebo se snižovat podle aktuálních potřeb."[3]

Stále více organizací reálné uvažuje o přesunutí části nebo i celého portfolia IT služeb do cloudového prostředí. A tedy tím začít využívat výhody, které cloudové platformy nabízejí. Jedním z předních poskytovatelů cloudových služeb je společnost Microsoft se svým produktem Azure. Tato diplomová práce se zaměřuje na návrh a realizaci migrace infrastruktury na platformě Microsoft Azure, a to s cílem zvýšit efektivitu, snížit náklady a zlepšit výkonnost organizace.

Pro ověřeni aktuálnosti tématu je do práce zahrnut i průzkum počtu odborných článků na téma migrace on premise infrastruktury do cloudu. Byla použita klíčová slova "migration, cloud, on premise, advantages, disadvantages"

Zde je uveden počet nalezených odkazů po letech ve formě grafu.



Obrázek 1: Publikace v letech

Práce prozkoumá postup migrace on premise infrastruktury do cloudového řešení. Konkrétně bude řešena migrace na platformu Microsoft Azure. Práce se na problematiku zaměří z různých úhlů pohledu, budou identifikované vhodné služby k migraci, naplánována samotná migrace a nakonec bude validováno a vyhodnoceno nové prostředí v cloudu.

2 Cíl práce

Cílem práce je poskytnout komplexní přehled o možnostech procesu migrace on premise infrastruktury do Microsoft Azure a navrhnout optimální postup založený na osvědčených praktikách a doporučených postupech. Analýza přínosu a rizik bude provedena pomocí SWOT analýzy a to včetně porovnání s alternativními řešeními, jako je udržení stávající infrastruktury nebo migrace na jinou cloudovou platformu. Tato diplomová práce je zaměřena prakticky a bude obsahovat studii situace imaginární organizace, která se rozhodla přesunout svou infrastrukturu do Azure. Budou popsány jednotlivé kroky takové migrace a jejich potencionální přínosy. Výsledky této práce mohou posloužit jako průvodce pro podobné organizace, které zvažují, nebo plánují přesun části nebo celé své infrastruktury do Azure. Zároveň přispěje k odbornému vývoji a získání přehledu o problematice migrace on premise infrastruktury do cloudu.

3 Metodika zpracování

V práci je použit postup, který začíná rešerší literatury, při které ověřuje, zda je téma relevantní a aktuální, dále rešerše slouží k nalezení zajímavých výsledků a zkušeností, ke kterým dospěli autoři předchozích prací.

Dále práce pokračuje analýzou možností cloudových technologií, a jak je potencionálně začlenit do infrastruktury podniku. Posuzuje jak nahradit, či přenést, a zda vůbec, konkrétní systémy podniku do cloudového prostředí.

Pomocí případové studie následně hledá možnosti jak takový přechod udělat, zda je efektivní a přínosný.

Práce tedy zodpoví několik otázek.

1. Je pro podnik přechod do cloudu efektivní a přínosný?
2. Jaké kroky jsou vhodné k úspěšnému přechodu do cloudu?
3. Jak řešit konkrétní on premise aplikace v cloudu?

První otázku práce zodpoví analýzou současných možností nabízených poskytovateli a jejich jednoduchým porovnáním s on premise možnostmi.

Druhou otázku vyřeší práce případovou studií, kde bude naznačeno, jak postupovat a jaké kroky v jakém pořadí je vhodné provést.

Třetí otázka bude zodpovězena v případové studii, ve které budou naznačena řešení přechodu vybraných, běžných on premise aplikací do cloudu.

4 Rešerše

Zajímavé téma řeší autoři Paulo Jorge Passos da Costaa, António Miguel Rosado da Cruz ve svém článku Migration to Windows Azure – "Analysis and Comparison z konference CENTERIS 2012."Článek je sice staršího data, ale téma je stále aktuální. Autoři nejprve představují koncept cloudu a jeho možnosti. Následuje případová studie, ve které popisují migraci menší aplikace z on premise prostředí do cloudu. Z jejich závěrů vyplývá, že přechod do cloudového prostředí nezpůsobil žádné zhoršení výkonu aplikace, naopak organizace dosáhla finančních úspor při nákupu hardwaru, softwarových licencí a také energií. Dále autoři zdůrazňují, že organizace získala přístup k prostředkům a službám, které jsou pro menší organizace často obtížně dosažitelné. Autoři rovněž diskutují o potenciálních nevýhodách, jako je bezpečnost a právní otázky spojené s ukládáním dat do cloudu.[3]

Nicméně, v dnešní době jsou tyto nevýhody překonány, neboť hlavní poskytovatelé cloudových služeb disponují mnoha mezinárodními bezpečnostními certifikacemi. Problematické otázky týkající se ukládání dat, včetně aspektů spojených s GDPR, jsou již dobře řešeny.

Další zajímavou prací je "Application Migration to Cloud: A Taxonomy of Critical Factors"autorů Van Tran, Jacky Keung, Anna Liu CSE, University of New South Wales, Australia The Hong Kong Polytechnic University, HKSAR National ICT Australia Ltd. Australia Thikhanhvan.Tran@nicta.com.au, Jacky.Keung@comp.polyu.edu.hk, Anna.Liu@nicta.com.au, Alan Fekete School of Information Technologies The University of Sydney, Australia. Alan.Fekete@sydney.edu.au ve které autoři řeší několik vzorových migrací on premise aplikací do cloudu. Rozdělují proces do logických úloh a stanovují užitečnou taxonomii jednotlivých úloh. Dále ukazují rozdělení nákladů na jednotlivé kategorie úloh. Zabývají se také dalšími důležitými faktory, které ovlivňují náklady na různé migrační úlohy. Celkově dává jejich práce organizacím možnost, jak stanovit náklady na migrace konkrétních aplikací a usnadnit jim rozhodování.[4]

Identifikací problému a úskalí, která mohou potkat organizace při migraci aplikací do cloudového prostředí se také zabývá práce autorů Mahdi Fahmideh University of New South Wales, Sydney, Australia Farhad Daneshgar University of New South Wales, Sydney, Australia Ghassan Beydoun University of Technology Sydney, Australia, Fethi Rabhi University of New South Wales, Sydney, Australia s názvem "Challenges in migrating legacy software systems to the cloud - an empirical study."autoři provádějí rešerši literatury, ze které vytvářejí model pro migraci legacy aplikací do cloudového prostředí, ten pak validují pomocí 104 vybraných a náhodně vybraných expertů z různých průmyslových odvětví. Pomocí statistické analýzy se jim daří model vytvořit, ale stále nechávají prostor pro jeho budoucí doplnění či úpravy dalším výzkumem.[5]

Konkrétní migrací na služby typu platform as a service se zabývá práce autorů R B Suryawan, R Ferdiana and Widyawan z Electrical and Information Technology Department, Gadjah Mada University, Yogyakarta, Indonesia."The Comparison of Cloud MigrationEffort on Platform as a Service."Autoři empiricky zkoumají migrace aplikace k různým poskytovatelům a provádějí zkušební migrace aplikace na variantu plafrom as a service u různých cloudových poskytovatelů a měří obtížnost takového procesu. Empirické výsledky ukazují, že Azure App Service a Amazon Elastic Beanstalk mají podobnou náročnost, zatímco Google App Engine má náročnost nejvyšší. Azure App Service (22 kroků) a Amazon Elastic Beanstalk (24 kroků) mají téměř stejnou náročnost a Google App Engine má mnohem vyšší (57 kroků). Rozdíl ve funkcích pro nasazování a podpoře platformy u jednotlivých dodavatelů cloudových služeb PaaS významně ovlivňuje náročnost migrace on premise aplikací do cloudového prostředí.[2]

Poslední prací uváděnou v této rešerši je "Advancements and approaches towards moving from legacy application to cloud"autorů Rashmi Rai* and G. Sahoo, Birla Institute of Technology, Mesra, India a Shabana Mehfuz Faculty of Electrical Engineering, Jamia Milia Islamia, New Delhi, India, kteří se zaměřuji na nedávné pokroky, ke kterým došlo při přechodu ze starších systémů na cloud. Práce rovněž zahrnuje pokroky v oblasti migrace virtuálních strojů. Autoři docházejí k závěru, že problematika cloudových řešení a migrací na ně, se vyvíjí velmi rychlým tempem a skýtá mnoho prostoru k výzkumu i pokroku. [6]

Provedením této rešerše je zjištěno, že k úspěšné migraci on premise prostředí a aplikaci do cloudu je nutné, aby organizace nepodcenily plánování a přípravu. Také vzhledem k dynamickému vývoji v cloudovém segmentu IT, je třeba klást důraz na trénink a vzdělávání zaměstnanců zodpovědných za migraci. Je nutné aby zodpovědní zaměstnanci měli vždy aktuální a celistvé informace a znalosti.

5 Nevýhody a omezení on premise a cloudové infrastruktury

Existuje několik nevýhod a omezení, které by měla organizace zvážit, před rozhodnutím provozovat on premise infrastrukturu.

Patři mezi ně například vysoké počáteční náklady na on premise infrastrukturu. Autoři Lynn Johnson, Cassandra Callaghan, Madhan Balasubramanian, Haris Haq, Heiko Spallek ve své studii "Cost Comparison of an on premise IT Solution with a Cloud-Based Solution for Electronic Health Records in a Dental School Clinic"zkoumají celkové náklady na vlastnictví Total cost of ownership - Celkové naklady na provoz a vlastnictví (TCO) na provozování zdravotnického informačního systému na lékařské fakultě. Posuzují provoz v cloudu oproti variantě provozu on premise. Byl porovnáván stávající on premise systém s variantou cloudového řešení. Autoři dospěli k nejenom finanční úspoře nákladů přibližné 2 mio dolaru během dvou let, ale identifikovali také mnohem širší prostor k inovacím a jejich snadnější implementaci v cloudu. [7]

On premise infrastruktura vyžaduje vysoké počáteční investice. Je nutné nakoupit hardware, software a další fyzická zařízení. Organizace pak následně musí provozovat servery, síťovou infrastrukturu, úložiště a další zařízení. Tyto náklady mohou být značně vysoké a je zde také riziko, že organizace špatně odhadne budoucí potřeby a investice tak může být zmařena.

Další nevýhodou v případě provozování on premise infrastruktury je, že se bude muset organizace potýkat s omezenými možnostmi škálování a flexibility.

"Místním zdrojům obvykle nelze snadno navyšovat nebo snižovat prostředky - i to vyžaduje určitý čas a investice."[8] Oproti cloudovému řešení musí organizace velmi dobře odhadnout budoucí potřeby, jinak se vystavuje riziku, že bude provozovat neefektivní a přehnaně dimenzovanou infrastrukturu, nebo naopak ji brzo přestanou zdroje stačit. Škálování v on premise prostředí je vždy náročnější a drahé. Snižovaní prostředků je v podstatě nemožné. Zbytečnou investici organizaci už nikdo nevrátí.

Také následná správa a administrace on premise infrastruktury je náročná a drahá. "Spolehlivá lokální infrastruktura vyžaduje značné investice, jako jsou náklady na aktualizaci a údržbu, pravidelné předplatné a výdaje na vlastní tým IT."[8] Organizace tedy musí investovat do vlastního IT týmu, který se stará o správu, údržbu, aktualizace a opravy infrastruktury. Samozřejmé nese veškeré náklady na jejich zaměstnávání, školení a správu on premise infrastruktury.

Další nevýhodou je starost o zabezpečení on premise infrastruktury. Organizace je plně odpovědná za bezpečnost. Musí zajistit vybudování a vyškolení týmu a prostředků jako jsou firewall, antivirový software, šifrování dat a pravidelné zálohování. Plně si zodpovídá za řešení bezpečnosti a jakékoliv útoky či incidenty na on premise infrastruktuře mohou mít fatální následky.

Také možnosti vybudování vysoce dostupné architektury nebo obnova po havárii bývá omezená. Pro organizace to znamená další nemalé investice do vybudování redundantních prostředků, geograficky oddělených datacenter a řešení pro zálohování dat. Dále potřebuje tým vyškolených lidí s náklady, které to sebou nese. Navíc se organizaci zvětšuje komplexita a složitost celé infrastruktury.

V neposlední řadě je to ztížený přístup k technologickým inovacím. Svět IT je extrémně dynamický a vyvíjí se opravdu rychle. Pro organizace může být poměrně obtížné on premise infrastrukturu na stejné technologické úrovni udržet. Navíc některá výpočetně náročná řešení, jako AI, strojové učení a podobně, mohou být na on premise infrastruktuře v podstatě

neprovozovatelná či dokonce neřešitelná. Organizace tak mohou ztrácet inovační potenciál a tím i konkurenční výhody.

Stejně tak ale i cloudová řešení, přestože nabízejí mnoho výhod, mají také určité nevýhody, které organizace musí pečlivě zvažovat.

Podle průzkumu prováděného společností Gartner považuje 51 % respondentů za největší nevýhodu cloudového řešení jeho menší spolehlivost a náchylnost k výpadkům než u řešení on premise. 26 % považuje za největší nevýhodu cloudových řešení menši bezpečnost z důvodu ukládání dat mimo organizaci, 16 % větší náročnost a komplexitu IT z důvodu práce s větším množstvím vendorů, a 8 % všechny zmíněné. [9]

Nazariy Hazdun ve svém článku pro časopis Forbes "Cloud Versus On Premises: Advantages And Disadvantages Of Both Models"uvádí jako nevýhody cloudového řešení:

- Závislost na internetu
- Bezpečnostní rizika
- Omezenou kontrolu nad výpočetními zdroji [8]

Jednou z klíčových nevýhod je závislost na internetovém připojení. Organizace musí mít k dispozici spolehlivé a vysoce kvalitní připojení k internetu, které je ideálně zálohováno. Společnost Gartner očekává že:

- Do roku 2025 bude 50 % nových nabídek bezpečného připojení sítí mít Software defined wide area network - Softwarové definovaná rozlehlá síť (SD-WAN), což je nárůst o 10 % oproti roku 2022.
- Do konce roku 2025 bude nejméně 30 % organizací využívat služby softwarově definovaného cloudového propojení (SDCI) pro připojení k poskytovatelům veřejných komunikačních služeb (CSP), což je nárůst oproti přibližně 10 % v roce 2020.
- Do roku 2026 bude 45 % podnikových poboček využívat pro připojení k síti Wide area network - Rozlehlá datová síť (WAN) pouze internetové služby. [10]

"Rostoucí využívání internetových služeb pro přenos WAN a nutí poskytovatele přehodnotit vlastní nabídku internetových služeb i rozsah partnerské spolupráce s místními poskytovateli internetových služeb pro větší geografický dosah a diferenciaci."[10]

Je tedy zřejmé, že internetová konektivita se stává jedním z klíčových prostředků pro chod každé organizace. A tato problematika se drží v popředí zájmu. V případě výpadku internetového připojení se organizace ocitá v obtížné situaci, kdy je zneschopněna provádět jakoukoli činnost v cloudovém prostředí. Aby minimalizovala negativní dopady takové situace, organizace by měla mít připravené alternativní záložní možnosti. To může zahrnovat například zavedení další internetové linky od jiného poskytovatele, aby byla zajištěna redundance připojení. Také je důležité, aby zaměstnanci byli proškoleni a obeznámeni s používáním individuálních alternativních připojení, jako je například mobilní telefon či jiné přenosné zařízení.

Další možností je vyřešení problematiky home office, která umožňuje zaměstnancům pracovat z domova v případě nedostupnosti kancelářských prostor. To však znamená, že systémy a aplikace v cloudovém prostředí musí být navrženy tak, aby byly autonomní a nezávislé na místních prostředcích organizace.

Existuji i další možnosti jak řešit konektivitu s cloudem. Jedná se ale už o enterprice řešení. Jde především o různá privátní připojeni cloudu, jako je například Azure Expresroute

společnosti Microsoft, která mají definovaná a zaručená Service level agreement - smluvně zaručena úroveň služby. (SLA).

"Azure ExpressRoute umožňuje vytvořit privátní propojení mezi datacentry Azure a infrastrukturou ve vlastních prostorách organizace. Připojení ExpressRoute nevyužívají veřejný internet, a proto jsou spolehlivější a rychlejší a mají nižší latenci než typická připojení přes internet. Pokud organizace použije připojení ExpressRoute k přenosu dat mezi místními systémy a Azure, může to v některých případech výrazně šetřit náklady. "[1]

Důkladná analýza závislosti na internetovém připojení je klíčová pro organizace, které zvažují přechod na cloudová řešení. Příprava na možné výpadky a zajištění dostupnosti internetu je zásadní pro zachování kontinuity podnikových operací a minimalizaci rizik spojených s cloudovým prostředím.

Při implementaci cloudových řešení se organizace také setkávají s právními aspekty a předpisy týkajícími se ochrany dat. "Organizace často manipulují s citlivými daty, jako jsou osobní údaje zaměstnanců nebo zákazníků, stejně jako s daty, která jsou právně hodně citlivá. Využívání cloudových řešení má řadu právních souvislostí a důsledků. Tyto důsledky jsou pochopitelně odlišné pro koncového uživatele, třeba vlastníka telefonu, a jiné pro banku nebo úřad, který využívá komplexní službu od dodavatele."[11]

"Pokud cloudovou službu využívá podnikatel nebo veřejnoprávní subjekt, je situace o poznání komplikovanější. Do hry totiž vstupuje řada dalších právních aspektů. Některé právní povinnosti, resp. okruhy, které je nutno uplatnit, jsou v zásadě stejné pro všechny organizace, další se však zásadně liší podle toho, o jaký subjekt se jedná. Jiné povinnosti totiž dopadají na výrobní podnik, který v cloudu provozuje jen e-mailové servery, jiné povinnosti na zdravotnická zařízení, jiné na banku a z velké části odlišné, či dodatečné povinnosti se uplatní i na subjekty veřejné správy. Nejen právní povinnosti při přechodu části dat či infrastruktury do cloudu pak ovlivňuje i otázka, zda je daná organizace povinnou osobou ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti."[11]

Evropská unie, stejně jako mnoho dalších zemí, upravuje tuto problematiku prostřednictvím zákonů a předpisů. Jedním z příkladů je známá Směrnice o ochraně osobních údajů (GDPR), která přísně upravuje způsob nakládání s osobními údaji. "V zásadě směrnice GDPR nutí podniky udělat si pořádek v datech, dbát o jejich bezpečnost a mít přehled o tom kdo s případnými osobními údaji nakládá a jak."[12] V případě používání cloudových řešení je důležité řešit zabezpečení dat, jejich šifrování a geografické umístění. Často je legislativou například požadováno, aby data zůstala v určitém teritoriu a nesměla opustit jeho hranice z důvodu dodržení příslušných právních předpisů.

Organizace se musí důkladně seznámit s právními předpisy a regulacemi, které se vztahují na jejich oblast působnosti, a zajistit, že jejich cloudové řešení splňuje požadavky těchto předpisů. Důraz musí být kladen na zabezpečení dat, transparentnost a dodržování předpisů, aby organizace minimalizovala riziko právních sankcí a zachovala důvěru svých zaměstnanců a zákazníků ve správu jejich citlivých dat.

Další aspekt, který organizace musí zohlednit, je sofistikovanost provozu a konfigurace cloudových služeb. Tato problematika se v mnohém liší od provozování infrastruktury on premise a vyžaduje takové dovednosti, které administrátoři nemusí mít. Cloudové prostředí má svá specifika, která se často liší mezi poskytovateli. Organizace by měla zajistit odborné školení svého týmu expertů na cloud, aby byla schopna plně využít všechny možnosti a efektivně spravovat cloudové služby. Pro menší organizace je také možností najmout si externího odborníka či konzultanta, který jim pomůže s implementací a správou cloudové infrastruktury.

Nevýhodou cloudového řešení je také potenciální "Vendor Lock-in". "Vendor lock-in je situace, kdy zákazník používající produkt nebo službu nemůže snadno přejít na konkurenční produkt nebo službu. To může být velký problém, protože to může omezit zákazníkovy možnosti volby a ztížit mu získání nejlepší možné hodnoty za jeho peníze."[13] Organizace by měla do svého rozhodovacího procesu zahrnout posouzení, zda se nestává příliš závislou na jediném dodavateli, zda má alespoň nějakou alternativu nebo zda je ochotna takovou závislost akceptovat. Je důležité provést analýzu rizik a vyhodnotit, jaká opatření jsou nezbytná pro minimalizaci rizik spojených s Vendor Lock-in. To může zahrnovat smluvní ujednání či hybridní cloudové řešení, které kombinuje různé dodavatele. Organizace by měla mít strategii a plán pro případné změny dodavatele nebo přechod na jinou platformu, aby minimalizovala negativní dopady Vendor Lock-in na své provozní procesy.

Závěrem této kapitoly se dá říci, že jak on premise, tak i cloudové řešení má svoje nevýhody. Je na každé organizaci, aby zvážila, které převažují a jaké bude pro ni nejvýhodnější řešení. Užitečná by mohla být například SWOT analýza, která bude také součástí případové studie.

"SWOT analýza je metoda, jejíž pomocí je možno identifikovat silné a slabé stránky, příležitosti a hrozby spojené s určitým projektem, typem podnikání, podnikatelským záměrem, politikou (ve smyslu opatření) apod. Jedná se o metodu analýzy užívanou především v marketingu, ale také např. při analýze a tvorbě politik (policy analysis). Umožňuje komplexně vyhodnotit fungování firmy, nalézt problémy nebo nové možnosti růstu. Je součástí strategického (dlouhodobého) plánování společnosti. Patří k základním metodám strategické analýzy, protože propojuje poznatky z více oblastí a umožňuje zvážit různé možnosti dalšího rozvoje organizace."[14]

6 Přínosy migrace do cloudového prostředí obecně

Tato kapitola se zaměří na přínosy změny on premise infrastruktury a prostředí na cloudové řešení. Je nesporné, že cloudové služby přinášejí mnoho výhod a tak se tato práce zaměří pouze na ty nejvýznamnější. Přínosy mohou podniku přinést nejen technické výhody, ale i ovlivnit pozitivně finanční či strategickou stránku provozu organizace.

Jako první zmíníme flexibilitu a škálovatelnost. Jedná se o jednu z hlavních výhod migrace do cloudového prostředí obecně.

"Cloudová řešení nabízejí uživatelům zdroje a služby na vyžádání. Organizace tak mohou nabízet své služby, bez neefektivního utrácení peněz za lokální zdroje a technická zařízeni. Cena závisí na tom, jak je infrastruktura využívaná, jak dlouho a jaký výkon je spotřebován, jak velká data jsou uložena."[15]

Poskytovatelé cloudových služeb nabízejí rozsáhlou škálu řešení, služeb a prostředků, které umožňuji organizacím sestavit si svoje řešení přesně v souladu s vlastními potřebami a možnostmi bez významných kompromisů nebo omezení. Navíc v cloudu existují možnosti jak prostředí rychle a s minimálními výpadky modifikovat podle aktuálních potřeb organizace. Je možné jednoduše a rychle pracovat s kapacitou. A to nejenom přidávat, ale i ubírat dle aktuálního zatíženi a potřeby. Vše je se dá ovládat i bezzásahově, pomocí automatických nástrojů. To umožňuje organizacím téměř okamžitě reagovat na změny prostředí nebo trhu a rychle plnit potřeby zákazníků. V neposlední řadě cloudová infrastruktura umožňuje provoz testovacích a vývojových prostředí bez výrazných investic do fyzické infrastruktury. Cloudové prostředí také přímo vybízí k zavedení Development and Operations (DevOps) praktik a tedy ke zlepšení procesů vývoje, nasazování a provozování aplikací. Úzké spolupráci provozních a vývojových týmů s nepřerušenou smyčkou vývoje, provozu a vylepšování provozovaných aplikací.

Další významnou výhodu je spolehlivost a dostupnost služeb provozovaných v cloudu.

"Cloudová řešení nabízejí Quality of services - smluvně zaručená kvalita služeb. (QoS) pro své uživatele, jako je šířka pásma, rychlost procesoru a dostupnost úložišť."[15]

Poskytovatelé cloudových řešení mají obvykle výkonná datové centra rozmístěná po celém světě. Tato data centra mají vysokou úroveň dostupnosti a zálohování. Disponují mnohonásobným připojením k internetu a vícenásobnou možností napájení energií. Mají pokročilý monitoring hardware a procesy jak zabránit náhodnému selhání hardwarových komponent. Tím je organizacím zaručena vysoká dostupnost a možnosti zálohováni systémů a významně se zkracuje Recovery time objective - Čas potřebý k obnově ze zálohy (RTO) po případné havárii. A zužuje se mezera Recovery point objective - Časový bod ze kterého je možné obnovit zálohu (RPO) snižující dobu za kterou dojde k případné ztrátě dat. Vzhledem k tomu, že zákaznická tolerance k nedostupnosti služeb se neustále snižuje a na trhu je velké množství konkurenčních organizací, které jsou schopné nedostupnou službu nahradit, stává se stabilita a spolehlivost služeb poskytované organizacemi, čím dál tím více důležitým faktorem a výhodou.

V neposlední radě je jednou z podstatných výhod snadná správa a aktualizace prostředků. Pokud organizace přesune služby do cloudu, podstatně to povede k omezení starosti o údržbu vlastní infrastruktury. Tyto starosti za organizaci zajistí poskytovatel cloudových služeb. Postará se o údržbu hardwaru, aktualizace operačních systémů a zajistí i bezpečnost. Tím organizaci zbude více prostoru pro zajištění obchodně významnějších činností a snížit náklady spojené s běžnou péčí o IT infrastrukturu.

"S tím ruku v ruce jde i snížení nákladů. Vzhledem k tomu, že poskytovatel cloudových služeb hradí veškeré náklady spojené s údržbou a správou serverů, mohou jejich klienti ušetřit prostředky, které by jinak utratili za vlastní datová centra."[8]

Pokud organizace provozuje vlastní infrastrukturu, musí investovat do vlastního hardware, software a lidských zdrojů. často je nucena postavit infrastrukturu, která dokáže pokrýt výkonové špičky, ale po zbytek času běží značně neefektivně. To může být zejména pro menší organizace finančně náročné. Cloudoví poskytovatelé často nabízejí možnosti placení pouze za spotřebovanou kapacitu a služby, což organizacím snižuje náklady. Ty pak mohou následně investovat finanční prostředky efektivněji, například do inovací a rozvoje své obchodní činnosti.

Jako poslední, ale neméně důležitou výhodou se budeme zabývat bezpečností. Poskytovatelé cloudu nabízejí mnoho funkcí a nástrojů pro zabezpečení dat, aplikací a infrastruktury. Bezpečnost je jedním z hlavních důvodů, proč organizace uvažují, nebo již začali využívat cloudových služeb. Významní poskytovatelé mají své cloudové služby certifikovány mezinárodními certifikacemi, Dávají k dispozici pokročilé nástroje na detekci hrozeb a útoků. Díky své velikosti mají podstatně vetší objem dat na které mohou své bezpečnostní systémy učit detekovat a bránit hrozbám. Mívají pokročilé služby pro správu identit, autorizaci a authentifikaci uživatelů. A to jak samotné organizace, tak i jejich zákazníků. Poskytují pokročilé nástroje pro zálohování a obnovu v případe havárie. V neposlední řadě i mnoho pokročilých nástrojů pro monitoring analýzu logů i jiných událostí. Organizacím se tak usnadňuje řešení bezpečnosti a zůstává prostor pro jiné obchodně zajímavější aktivity.

"Například Azure nabízí více než 100 certifikací dodržování předpisů, včetně více než 50-ti certifikací pro konkrétní globální oblasti a země, včetně USA, Evropské unie, Německa, Japonska, Spojeného království, Indie a Číny."[1]

7 Případová studie

"Přesun stávajících starších systémů na cloudové platformy je náročný a nákladný proces, který může zahrnovat technické i netechnické zdroje a problémy. Existují důkazy, že za mnoha neúspěchy migrace při dosahování cílů organizací stojí nedostatečné pochopení a nepřipravenost migrace na cloudové služby."[5]

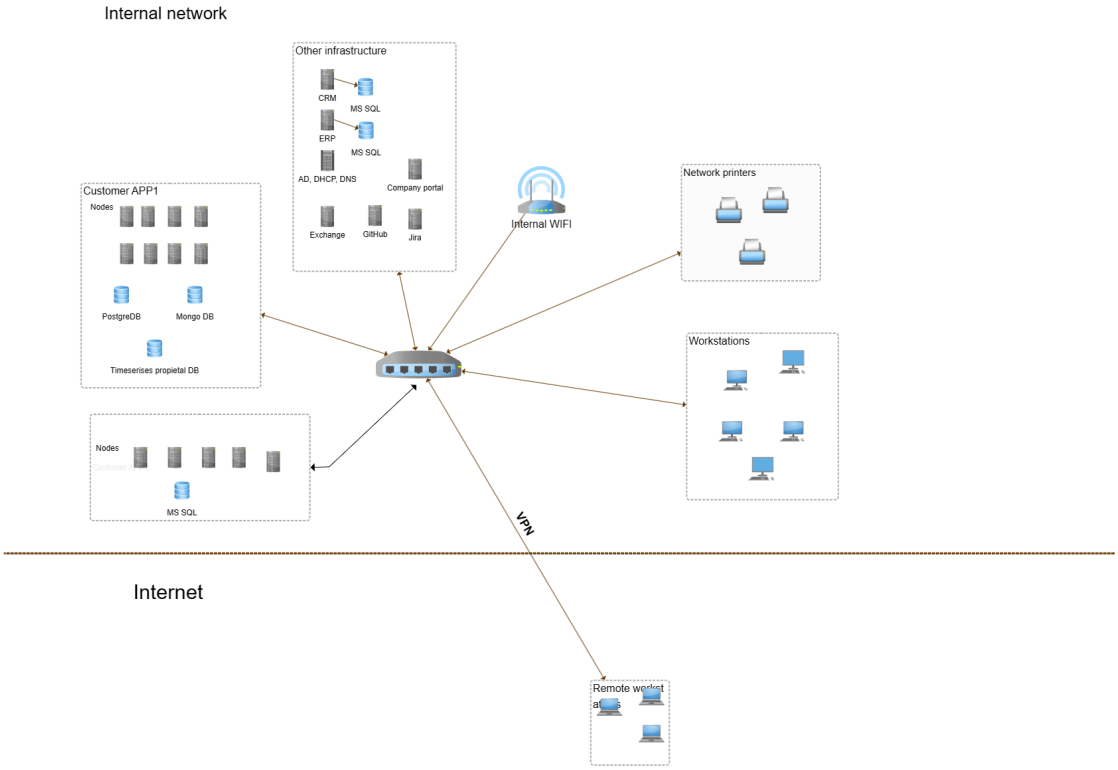
Tato studie se pokusí poskytnout návod jak se neúspěchu vyhnout a projít procesem migrace k úspěšnému konci.

Jako modelový příklad budeme uvažovat organizaci ze soukromého sektoru o střední velikosti 500 zaměstnanců. Společnost produkuje Programmable logic controller - programovatelný logický automat. (PLC) moduly, které následně řídí různé stroje a zařízeni u zákazníků. Tyto moduly lze monitorovat a ovládat i vzdáleně. V současné době má organizace pobočky po celém světě a na její IT služby jsou kladeny čím dál tím vetší nároky. Organizace postupně rostla a s ní i její IT. Současné on premise řešení už naráží na svoje limity. Organizace tedy jako jedno z možných řešení zvolila migraci služeb do cloudového řešení. Jedná se zejména o online monitorovací systém jednotek, Customers relatioship management - Nástroj řízeni vztahů se zákazníky (CRM), Enterprice resource plannig - Nástroj pro plánováni zdrojů (ERP), ale také nástroje pro vývojáře jako je verzovací systém nebo nástroje pro vedení projektu.

Tabulka 1: Přehled služeb organizace

Služby	Aktuální prostředky	počet
Active Directory	Windows server AD, DNS, DHCP	1
File share server	Windows server	0
Print sharing	Windows server	0
Mail server	Windows serrver, MS Exchange	1
Jira	Linux server, Jira	1
GitHub	Linux server, GitHub	1
CRM	Windows server, SQL database	2
ERP	Windows server, SQL database	2
Company portal	Windows server, IIS, SQL database Kentico	1
Customer app1	Windows server, IIS, SQL database, .Net services	8
Customer app2	Windows server, IIS, SQL database	5

Z výše uvedené tabulky vyplývá převaha MS technologii v organizaci. Z tohoto důvodu se migrace do Cloudu Azure zdá být vhodná. On premise technologie Microsoftu jsou pro Azure nativní a on premise technologie mají svůj protějšek jako službu Azure. Také řízeni uživatelů a jejich práv je řešeno v Azure pomocí technologie Active directory a její propojení se stávající on premise instancí organizace je možné a uživatelé včetně práv budou převzaty do Azure AD.



Obrázek 2: Výchozí stav infrastruktury organizace - schema

7.1 Možnosti a servisní modely Microsoft Azure

Microsoft Azure nabízí mnoho servisních modelů a možností jak jím poskytované služby konzumovat.

Jedním z nejzákladnějších modelů je jednoduše si pronajmout hardware jako Infrastructure as a service - Hardware poskytovaný jako služba (IaaS), a provozovat si virtuální servery. V tomto případě je migrace stávajících serverů poměrně snadná, organizace mají servery plně pod kontrolou a existují nástroje, jak fyzické, či on premise servery snadno migrovat do cloudu. Organizace tak získá výhody zabezpečeného datového centra, nicméně bude pořád nutné o servery pečovat, stejně jako v on premise prostředí, Tedy je zálohovat, aktualizovat a administrovat.

"Vyšší úrovní abstrakce je Platform as a service - Platfroma poskytovaná jako služba (PaaS). PaaS je úplné prostředí pro vývoj a nasazení v cloudu, které organizaci poskytuje prostředky umožňující dodat cokoli od jednoduchých cloudových aplikací po propracované podnikové aplikace s podporou cloudu. Potřebné prostředky nakupujete od poskytovatele cloudových služeb na základě průběžných plateb a přistupujete k nim přes zabezpečené internetové připojení."[1]

V tomto případe organizaci odpadá starost o vrstvu hardware, operačního systému a potřebných engine. Organizace se soustředí pouze na vývoj a nasazování aplikací. O zbytek infrastruktury se stará samotný Azure. Jde zejména o platformu pro provoz webových aplikací, různé databáze, kontejnery a jejich správu a další.

"Úplně nejvyšší formou abstrakce infrastruktury je služba Software as a service - Aplikace poskytovaná jako služba (SaaS). SaaS poskytuje úplné softwarové řešení, které zakoupíte na základě průběžných plateb od poskytovatele cloudové služby. Pronajímáte si pro organizaci možnost použití aplikace a uživatelé se k ní připojují přes internet obvykle pomocí webového prohlížeče. Veškerá podpůrná infrastruktura, middleware, software a data aplikace jsou umístěné v datovém centru poskytovatele služeb. Poskytovatel služeb spravuje hardware a software a v rámci příslušné smlouvy o poskytování služeb zajišťuje dostupnost a zabezpečení aplikace a vašich dat. SaaS dovoluje vaší organizaci začít aplikaci rychle využívat s minimálními pořizovacími náklady."[1]

Tedy nabízí organizacím hotová řešení v cloudu a organizace se v podstatě vůbec nestará o infrastrukturu, aktualizace, zálohování, atd. Pouze řeší běžnou administraci používaného produktu. Příklady takových služeb jsou Office 365, Dynamics 365, ale i produkty třetích stran

Mezi další možnosti, které Azure nabízí patří definice infrastruktury v kódu, tedy Infrastructure as Code - Definování infrastruktury pomocí kódu (IaC). V podstatě umožňuje organizacím definovat a následně buildovat svojí infrastrukturu v cloudu pomocí kódu, například Terraformových šablon. Takové definice je možné následně držet v Gitu, verzovat kód, automaticky deployovat, zařadit do deployovacích pipelines atd. Jendou v podstatných výhod je, že šablony je, za cenu menších úprav, možné použit i v cloudech jiných poskytovatelů. mimo jiné jsou tedy velmi užitečné jako součást díssater recovery procesů.

V poslední části této kapitoly bude práce zaměřena na možné finanční modely, které Azure nabízí. V zasadě jsou dvě hlavní možnosti, jak za používaní služeb Microsoft Azure platit. První je Pay as you Go, tedy platba za aktuálně spotřebované prostředky. Tato varianta bývá zpravidla na kontinuální provoz poměrně drahá a hodí se spíše pro vývoj a testování, kdy prostředky nejsou požadovány kontinuálně. Organizace by měla ale dbát na to, aby byly, i v případě kdy není potřeba, vypínány nebo snižován jejich výkon. To vše cloudová řešení umožňují a je možné tak šetřit prostředky organizace

Další možností jsou formy různých předplatných na jeden a více let. Tato možnost je vhodná v situacích, kdy má organizace rámcovou představu, jaké prostředky bude do budoucna potřebovat a využívat a může se tak zavázat, že je vyčerpá. Azure pro takové případy poskytuje významné slevy. A povinnost čerpání nebývá vázána na konkretní instance služeb, ale na celkový balík. Tedy např ne na konkretní SQL server, ale na Všechny SQL servery, které organizace provozuje. Tedy, co nevyčerpá jeden mohou vyčerpat ostatní. V případě nepředvídatelné potřeby navyšovat výkon, je zde pořád možné využít variantu Pay as you go nebo navýšit závazek.

Organizacím se také může vyplatit možnost uplatnit stávající softwarové licence v Azure. Pokud již takové vlastní a licenční podmínky to umožňují (nejsou například OEM), tak se taková licence dá použít v Azure a není nutné za ně znovu platit.

Tabulka 2: Přehled servisních modelů [2]

Service Model	Popis	Uživatelem ovládané zdroje
Software as a Service (SaaS)	Zákazník používá aplikace, které provider provozuje sám v cloudu	Pouze uživatelská nastavení.
Platform as a Service (PaaS)	Zákazník deployuje do cloudu nad podporované prostředím poskytovatele aplikaci	aplikace Uživatel má kontrolu deployment procesem a některými konfiguracemi prostředí
Infrastructure as a Service (IaaS)	Zákazník si může instalovat libovolný software včetně operačního systému. Využívá úložiště, síť a ostatní výpočetní prostředky poskytované providerem	Uživatel má kontrolu nad operačním systémem, úložištěm a deploymentem aplikací, Dále má možnost kontrolovat sítové komponenty jako Firewally apod.

7.2 Plánování a realizace migrace do Microsoft Azure

Úspěšný přechod z on premise infrastruktury na cloudové služby vyžaduje pečlivé naplánování. Organizace musí zvážit jaké aplikace a v jakém pořadí bude migrovat. Úspěšným plánováním migrace do cloudového prostředí se zabývá například článek Application Migration to Cloud: A Taxonomy of Critical Factors autorů Van Tran, Jacky Keung, Anna Liu CSE, University of New South Wales, Australia The Hong Kong Polytechnic University, HKSAR National ICT Australia Ltd. Australia Thikhanhvan.Tran@nicta.com.au, Jacky.Keung@comp.polyu.edu.hk, Anna.Liu@nicta.com.au Alan Fekete School of Information Technologies The University of Sydney, Australia Alan.Fekete@sydney.edu.au kde shrnují poznatky migrace několika vzorových aplikací a navrhují povedenou taxonomii migračních úkonů a rozdělení nákladů. Autorům se podaří identifikovat důležité faktory ovlivňující náklady na migraci do Cloudu, což poskytuje základ pro sestavení modelu odhadu nákladů speciálně přizpůsobeného pro Cloudové služby. [4]

Při plánování musí organizace zohlednit kritičnost aplikací, jak dlouhý výpadek je pro ně přípustný. Jak budou procesy fungovat v přechodném období. Dále jak bude celý proces sledovat a nakonec vyhodnocovat. Také je vhodné mít dopředu připravené procesy na provoz infrastruktury v cloudu a vyškoleny příslušné lidi. Jednou z vhodných součástí rozhodovacího procesu je také SWOT analýza, která nám pomůže udělat si Přehled o silných a slabých stránkách, příležitostech a hrozbách. níže jsou uvedené příklady takové analýzy.

Tabulka 3: SWOT analýza přechodu organizace do cloudu obecně

Silné stávající IT	Nedostatečná znalost cloudových technologii
Podpora přechodu do cloudu vedením	Standartní internetové připojení s nedostatečným SLA
Zavedena kultura HomeOffice	Nedůvěra některých zaměstnanců
Zlepšení možností inovací	Závislost na internetové lince
Prostředky k dispozici on demand	Hrozba Vendor lock-in
Zlepšení řízeni security	Hůře předvídatelné náklady

Tabulka 4: SWOT analýza přechodu do Azure

Nativní prostředí MS stejné jako v organizaci	Podpora pouze taková jaká je zaplacena.
Široká technická podpora produktů	Vybrané služby mohou být dražší.
Certifikace a bezpečnost	Menši nabídka poskytovaných služeb
Jednotné prostředí pro řízeni uživatelů a oprávnění	Žádná kontrola nad fyzickým HW
Zlepšení kooperace zaměstnanců pomocí nástrojů Azure	Nedostatečně vyškolený IT tým A
Úspora prostředků a času věnovaného operations IT	Vendor Lock-in

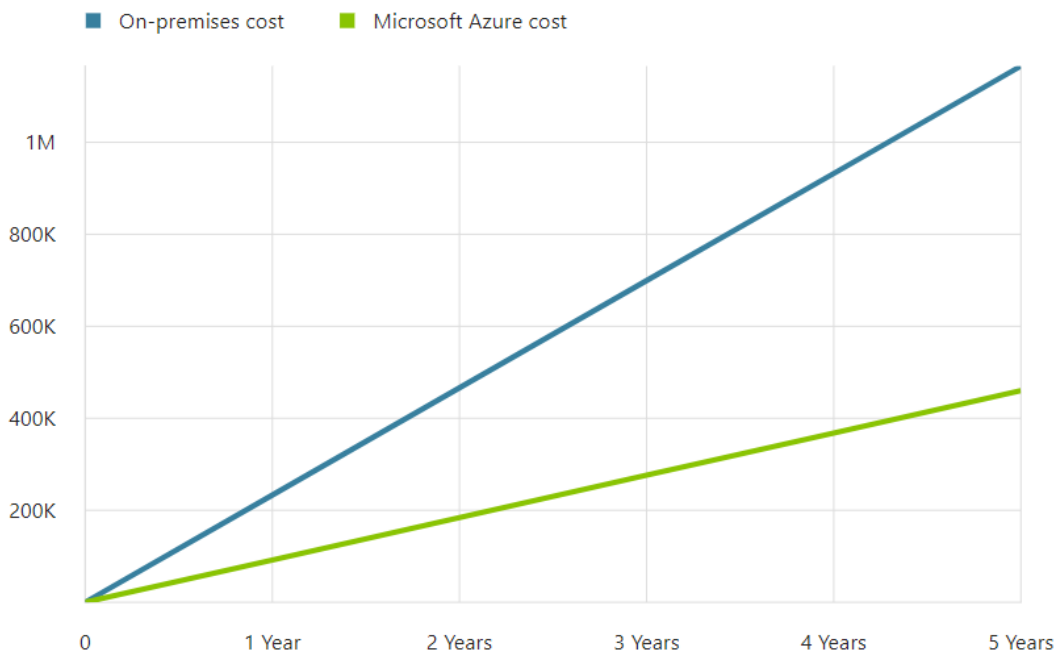
Součástí přípravné fáze by měla být i analýza TCO, aby organizace měli jistotu, že přechod do Azure bude pro ně efektivní i z pohledu nákladů. V této práci je pro případové studii použit TCO kalkulátor poskytovaný společností Microsoft. Tento nástroj umožní organizaci udělat si přehled o očekávaných nákladech přechodu do cloudu a porovnat si je s předpokládanými náklady provozu infrastruktury on premise.

V TCO kalkulátoru byly zvažovány následující hardwarové prostředky

Tabulka 5: HW prostředky uvažované k přesunu do Azure

HW	Funkce	Počet
Server 1 x CPU/4 Core 312 GB RAM	ERP, CRM App	2
Server 1 x CPU/2 Core 256 GB RAM	GitHub	1
Server 1 x CPU/4 Core 448 GB RAM	Customer app 1	8
Server 2 x CPU/4 Core 256 GB RAM	Customer app 2	5
Web app 1 x CPU/2 Core 448 GB RAM	Company web	1-3
SQL database std. 2 x CPU/4 Core 448 GB RAM	SQL databáze	2
Storage 10 TB	Úložiště	1
Backup 10 TB	Záloha dat	1
Archiv 10 TB	Archiv dat	1
Síťové připojení 1 GBps	Připojení do Azure	1

Dále byly v kalkulátoru uvažovány průměrné ceny elektřiny za 1 kWh v Evropě a průměrné ceny HW a práce stanovené společností Microsoft. Tyto parametry lze však v kalkulátoru upravovat podle aktuální, nebo místní situace. Jak je vidět z grafu a tabulky dále převodem zadané infrastruktury do cloudu Azure je možná úspora až 705 458 Eur během pěti let. Celý report je přiložen k práci jako příloha A



Obrázek 3: Graf rozdílu TCO v on premise vs. Azure

On-premises cost breakdown summary		Azure cost breakdown summary	
Category	**Cost**	**Category**	**Cost**
Compute	$1,009,293.00	Compute	$430,058.04
Hardware	$379,952.00	Data Center	$0.00
Software	$492,400.00	Networking	$0.00
Electricity	$56,653.80	Storage	$41,349.12
Database	$80,287.20	IT Labor	$30,667.05
Data Center	$78,590.20		
Networking	$150,489.72		
Storage	$3,712.00		
IT Labor	$43,700.00		
Total	**$1,285,785.00**	**Total**	**$502,074.00**

Obrázek 4: Sumarizace rozdílu TCO v on premise vs. Azure

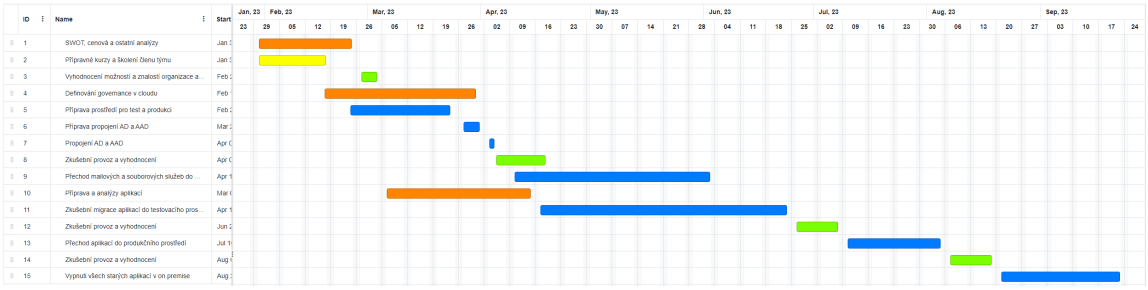
Po ověření, že migrace do cloudu bude pro organizaci přínosná je vhodné pokračovat přípravou plánu přechodu. V tomto plánu je seznam kroků, které je nutné učinit k úspěšné realizaci přechodu organizace do cloudu. Dále je nutné určit příslušné týmy zodpovědné za jednotlivé kroky a připravit časový plán a návaznosti kroků. Jedním z nástrojů může být například Ganttův diagram.

"Ganttův diagram byl vytvořen už v roce 1896 Karolem Adamieckim, který ovšem svůj výtvor publikoval až po Henrym L. Ganttovy. Diagram znázorňuje časový průběh několika činností, které mohou probíhat paralelně. "[**?**]

Vzhledem k tomu, že tato práce se zaměřuje na technické řešení přechodu on premise infrastruktury do cloudu je jako příklad pro tuto případovou studii uvedena zjednodušená forma takového plánu a Ganttova diagramu. Jednotlivé kroky obsahují odhady časové náročnosti v Man day's - Jednotka práce odvedené jedním člověkem za den. (MD). Kvalifikované odhady vycházejí z praxe autora, který se na několika migracích podílel. Kroky jsou v tabulce uvedeny tak, jak by měli jít za sebou.

Tabulka 6: Plán přechodu organizace do cloudu

Krok	Časová náročnost - odhad v MD
SWOT, cenová a ostatní analýzy	20
Přípravné kurzy a školení členu týmu	50
Vyhodnocení možností a znalostí organizace a členů týmu	5
Definování governance v cloudu	30
Příprava prostředí pro test a produkci	20
Příprava propojení AD a AAD	5
Propojení AD a AAD	2
Zkušební provoz a vyhodnocení	10
Přechod mailových a souborových služeb do O365	80
Příprava a analýzy aplikací	60
Zkušební migrace aplikací do testovacího prostředí	150
Zkušební provoz a vyhodnocení	10
Přechod aplikací do produkčního prostředí	50
Zkušební provoz a vyhodnocení	10
Vypnuti všech starých aplikací v on premise	10



Obrázek 5: Ukázka Ganttova diagramu

7.2.1 Vnější perimetr, připojení a jejich bezpečnost

Při přechodu organizace na cloudové služby přibude z pohledu bezpečnosti ještě péče o bezpečnost v cloudu. Azure však nabízí několik řešení, jak zabezpečit data a aplikace v Azure provozované. Výhodou bezpečnostních řešení v cloudu je, že provozovatel cloudu se setkává s mnohem větším vzorkem útoků, než běžné organizace, a je to pro něj příležitost, jak zdokonalovat svoje bezpečnostní procedury a systémy.

Základním bezpečnostním prvkem je Azure Firewall. Jedná se centralizovanou síťovou ochrannou službu, která poskytuje firewall a Network address translation - překlad síťových

adres. (NAT) pro ochranu vašich aplikací a sítí v Azure. Pomocí Azure Firewall je možné definovat a spravovat síťová pravidla pro řízení provozu mezi sítěmi.

Pokročilejším bezpečnostním prvkem, nejenom pro vnější perimetr v Azure je Web Application Firewall. Jedná se o aplikační firewall, chrání před nejrozšířenějšími hrozbami jako jsou SQL injection, Cross-site scripting. (XSS)), nebo ochrana proti botům, dále umožňuje také konfigurovat vlastní sadu bezpečnostních pravidel. Web application firewall analyzuje síťový provoz a blokuje potencionálně nechtěný provoz. Organizace má k dispozici sadu definovaných a aktualizovaných pravidel reagujících na aktuální bezpečnostní hrozby, dále si může definovat vlastní pravidla dle potřeby.

Oba tyto prvky je možné integrovat do flow ve službě Azure Front Door classic. Jedná se o globální škálovatelný vstupní bod, který je možné využít k zpřístupnění webových aplikací, či různých API z internetu. Je možné v něm integrovat jak Azure firewall, Web application firewall, tak i například Load balancer, pokud je taková potřeba. Front Door classic organizaci poskytne jednotný vstupní bod pro zákazníky.

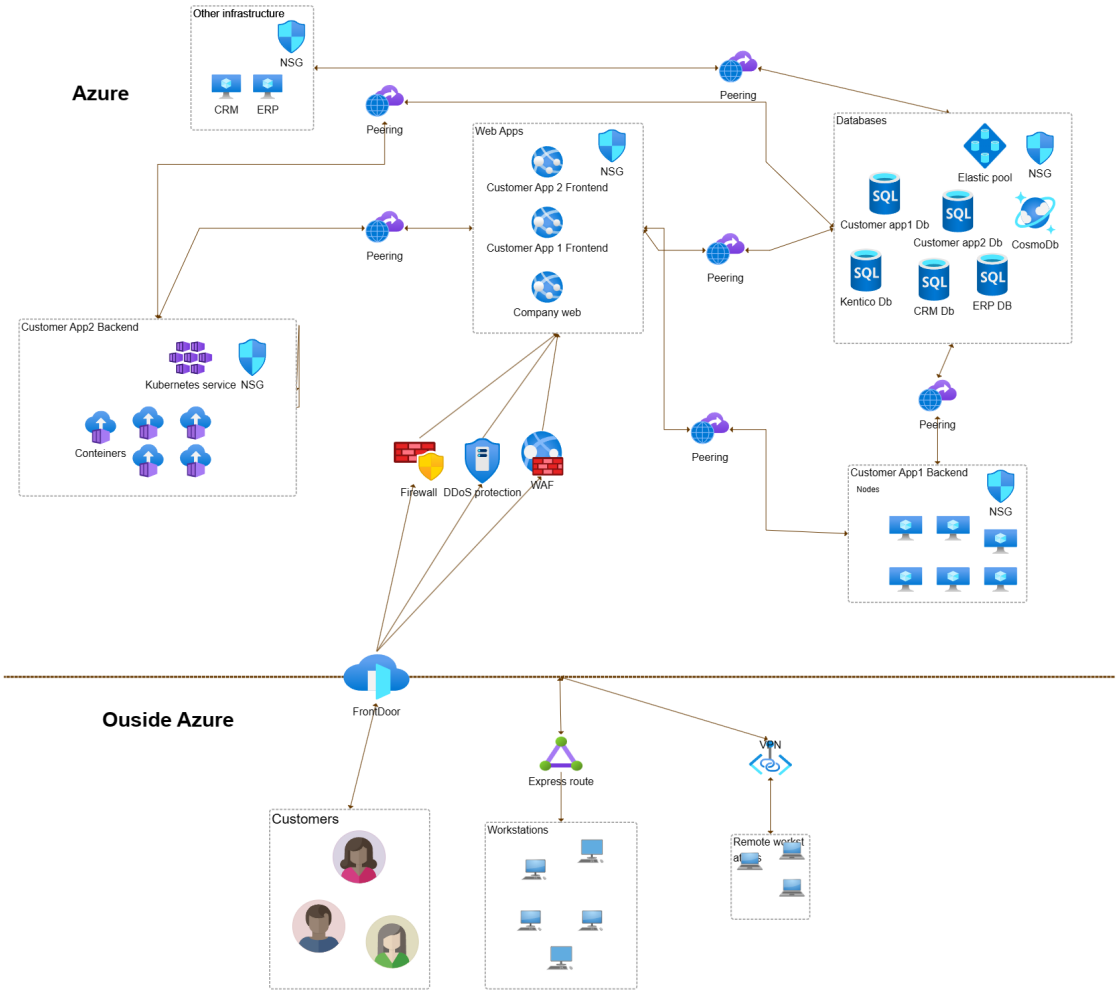
"Azure Front Door (classic) je globální, škálovatelný vstupní bod, který využívá globální okrajovou síť společnosti Microsoft k vytváření rychlých, bezpečných a široce škálovatelných webových aplikací. S Front Door (classic) můžete přeměnit své globální spotřebitelské a podnikové aplikace na robustní, vysoce výkonné personalizované moderní aplikace s obsahem, který se prostřednictvím Azure dostane k celosvětovému publiku."[16]

Poměrně častým útokem bývá Distributed denial of service - distribuované odepření služby. (DDoS), tedy úmyslné zahlcení prostředku dotazy a vyčerpání jeho možností, což v konečném důsledku znamená odepření služby zákazníkům. "Útok DDoS je zaměřen na znepřístupnění zdroje (stránky, aplikace, serveru) pro účel, pro který byl navržen."[17]

K potlačení tohoto typy útoku cloud Azure disponuje službou Azure DDoS protection. Služba automaticky monitoruje síťový provoz a reaguje na možné DDoS útoky.

Nakonec v případech, kde je to vhodné, je možné využít služeb poskytující izolované přístupové kanály ke službám, jako je například Azure private link, poskytující zabezpečení a privátní přístup přes privátní připojení, nebo Azure virtual network, který izoluje přístup z veřejného internetu a umožní přístup pouze z vnitřní sítě organizace.

V případové studii jako řešení pro potřeby organizace je zvažováno následující řešení. Zákaznické aplikace, webové stránky a zákaznická API společnosti budou zpřístupněny do veřejného internetu pomocí služby Front door classic. Bude implementována Web application firewall i firewall. Dále bude zařazen load ballancer, který bude balancovat provoz pro webové aplikace. Přístupy z organizace na interní aplikace budou řešeny pomocí služby Express route. Přistupy pracovníků mimo fyzické kanceláře budou realizovány pomocí Virtual private enetwork - virtuální privátní síť. (VPN) Níže je schématický obrázek takového řešení přístupových bodů.



Obrázek 6: Návrh řešení v Azure

7.2.2 Aplikační vrstva

Nejprve je potřeba aplikace, které organizace využívá, rozdělit na aplikace, které organizace nakupuje jako hotové programy, typicky třeba účetní systém, nebo systém pro správu zákazníků a aplikace, které si organizace vyvíjí sama ev. si vývoj řídí s pomocí subdodávek. V prvním případě Azure nabízí mnoho běžných aplikací jako cloudovou variantu přímo v Azure marketplace v režimu SaaS. Je tedy možné přejít na tuto variantu z on premise. Nicméně vyřešení problematiky licence a správy cloudové varianty si musí organizace vyřešit přímo s poskytovatelem aplikace. Azure v této variantě poskytuje pouze infrastrukturu na které aplikace běží.

Pokud neexistuje varianta aplikace uzpůsobená pro cloud a nabízena v Azure marketplace, je možné jí spustit na plnohodnotném virtuálním serveru se všemi výhodami a nevýhodami, jaké takové řešení má. Zde zase zůstává veškerá starost o provoz aplikace na bedrech organizace samotné a Azure poskytuje pouze infrastrukturu pro běh aplikace.

V případě, že organizace provozuje vlastní, například zákaznické aplikace, je v Azure několik možností, jak stejnou službu zákazníkům poskytnout jako cloudové řešení. Zde už záleží na konkretním případu užití jaká služba se v cloudu hodí.

Jednou z takových služeb je Web application service, jedná se o škálovatelnou službu umožňující provozovat webové aplikace. Podporuje různé programovací jazyky, jako je .NET, Java, Python, Node.js atd. Vývojáři tak mohou pracovat ve svém oblíbeném frameworku. Zároveň nasazovaní je poměrně snadné a například z Visual studia i automatizované. Také je poměrně dobře vyřešené škálování, které je možné i automaticky řídit na základě triggerů jako je aktuální zátěž CPU, paměti nebo podle počtu požadavků. Podporuje snadné připojení k běžným databázím včetně databázových služeb v Azure. [16]

Azure také podporuje kontejnerizaci aplikací, konkretně se jedná o službu Azure Kubernetes service, která zajišťuje kompletní správu kontejnerů, včetně monitoringu, úložiště obrazů kontejnerů a dalších. Je plně integrován s nástroji DevOps viz. kapitola "7.4 Vývoj a nasazováni v cloudu".

Další možností je Azure Functions pro vytváření serverless funkcí. Je ideální pro hostování kratších částí kódu nebo skriptu bez nutnosti spravovat infrastrukturu. Tyto kódy je možné spouštět na základě událostí, například http požadavku nebo harmonogramu. Tedy běží a jsou účtovány pouze v okamžiku, kdy jsou reálně potřeba.

"Azure Functions také podporují více programovacích jazyků, včetně C#, Java, JavaScript, Python, PowerShell a TypeScript. Jejich integrace s dalšími službami v Azure umožňuje propojení s dalšími částmi aplikace nebo systému a vytvářet tak celý funkční celek. Funkce je možné automaticky škálovat na základě zátěže. Jednotlivé funkce je možné sdružovat do logických celků pomocí služby Functions apps a mít tak jednotné prostředí pro nasazování a správu funkcí."[16]

V případě potřeby vytvářet automatické toky dat nebo pracovní postupy, je možné využít službu Logic apps. V této službě je možné pomocí grafického rozhraní takové postupy, integrace a automatizace vytvářet. Podporovány jsou služby Azure, SaaS aplikace ale i vlastní vytvořené aplikace. Největší výhodou logic apps je možnost plně konfigurovatelných spouštěčů akcí. Je možné použit časovače, webhooky, změny v úložišti, reagovat na příchozí emaily a další. [16]

Pro zasílání a správu zpráv zasílaných mezi různými částmi systému je možné použit plně spravovanou službu Azure Service Bus. Tato služba zprostředkovává odesílání a příjem zpráv mezi různými komponentami. Podporuje fronty, témata a odběry, a umožňuje spolehlivý a asynchronní přenos zpráv mezi aplikacemi. Podporovany jsou i pokročilé služby, jako je přesměrování zpráv mezi instancemi Service Bus nebo jiných služeb Azure. Azure Service Bus také disponuje širokými možnostmi sledování stavu zpráv, zajištění doručení zpráv na správná místa.[16]

V dnešní době je stále důležitější práce s daty a jejich snadné zpřístupnění ke strojovému zpracování. K tomuto účelu se v Azure dá využit služba Azure API Management, která umožňuje vytvářet, zabezpečovat a spravovat různé API ať už pro privátní nebo i veřejné využití. Jedná se o centralizované místo kde je možné vytvářet, publikovat API, zajistit autentizaci i autorizaci jejich uživatelů a analyzovat provoz na různých API. Součásti API managementu je i portál s dokumentací a správou účtu uživatele a testovacím prostředím. Dále je na API managementu možné pomocí politik data upravovat a přizpůsobovat pro koncové systémy, je tak možné přenášet data i mezi systémy, které nemají kompatibilní datový model.

Posledními dvěma službami, které je vhodné zmínit v této souvislosti, jsou Azure Content Delivery Network (CDN) a Azure IoT Hub.

Azure Content Delivery Network (CDN) je služba, která umožňuje efektivní a rychlé doručování obsahu. Využívá se zejména k doručeni statického obsahu, jako jsou obrázky, videa atd. CDN si naklonuje tento obsah na různá geograficky oddělená místa a dokáže následně zajistit doručení statického obsahu z geograficky nejbližšího serveru k uživateli. To vede k rychlejší odezvě a v důsledku ke zlepšeni uživatelské zkušenosti. Podporuje také různé optimalizace jako je různé cachování, komprimace obsahu apod. To vede ke zmenšení objemu dat a dalšímu zrychlení doručení dat uživateli. Azure CDN je globálně dostupná služba, má pokrytí v regionech a datových centrech po celém světě.

IoT hub je plně spravovaná platforma pro správu a komunikaci s velkým množstvím IoT zařízení. Podporuje protokoly MQTT, AMQP a HTTPS a umožňuje dvoucestnou komunikaci. Je možné ho integrovat do analytických nástrojů a analyzovat či vizualizovat tak data.

Pro účely případové studie bude aplikační vrstva řešena následovně. Základní služby jako je mail, Teams, sdílení souboru bude řešena službou Microsft 365, který v sobě zahrnuje několik SaaS aplikací. Organizace tedy využije zejména produkty Exchange, Temas, One drive a Office 365. Tím bude mít vyřešenu problematiku poštovních služeb, bezpečné platformy pro sdíleni dat a instant messagingu.

Organizace dále provozuje ERP a CRM systému postavený na platformě Microsoft Dynamics. Společnost Microsoft poskytuje cloudovou SaaS službu Dynamics 365. Stávající CRM a ERP systémy budou analyzovány a případně převedeny na tuto variantu. Pokud převod nebude možný, bude CRM a ERP nadále provozován na virtuálních serverech v Azure.

Verzovací systém GIT bude řešen v rámci Azure DevOps, které budou blíže rozebrány v kapitole "7.3 Správa a optimalizace cloudového prostředí"

Systém pro projektové řízeni Jira bude řešen jako SaaS služba Jira cloud od společnosti Atlassian. V Azure není efektivní cesta jak aplikaci Jira provozovat. řešení pomocí virtuálních strojů v situaci, kdy společnost Atlassian přestává on premise instalace podporovat je značně neefektivní, zejména když společnost Atlassian nabízí vlastni SaaS produkt Jira cloud.

Organizace dále potřebuje řešit Company protál, jedná se o .Net webovou prezentaci společnosti, která umožňuje zákazníkům registrovat se a zobrazit si pro sebe relevantní údaje jako je např, záruka na zakoupené produkty. Tyto data jsou získávaný ze sytému ERP a CRM. Webová prezentace bude převedena na PaaS službu Azure Web Application. Datová integrace bude zajištěna službami Azure Service Bus a API Management.

Jako poslední organizace potřebuje převést do cloudu dvě zákaznické aplikace, které slouží k monitoringu a správě zakoupených produktů. Jedná se o hlavní a podpůrnou webovou aplikaci. Hlavni web aplikace "Customer app 1"obsahuje Frontend a Backend část. Frontend část bude převedena na PaaS službu Azure Web Apllication. Backend bude analyzován a do cloudu převeden na služby Azure web Application, Azure Function, Logic Apps a Virtual server.

Podpůrná aplikace "Customer app 2"Získává ověřená data z veřejných zdrojů a poskytuje je hlavní aplikaci k vyhodnocení. Tato aplikace bude převedena do Docker kontejnerů a provozována ve službě Azure Kubernetes Services.

Statický obsah všech frontendů bude umístěn do sítí CDN a bude tak zjištěn efektivní a rychlý přístup zákazníků k těmto datům z celého světa.

7.2.3 Ukládání dat

Klíčovým aspektem moderních aplikací je datová persistence. Data hrají v organizaci často klíčovou roli a jsou mnohdy vysoce ceněna. Azure poskytuje několik služeb a nástrojů pro spolehlivé, bezpečné a efektivní ukládáni dat.

Prvním z nich je Blob storage. Jedná se o úložiště nestrukturovaných dat o velkých objemech, jako jsou obrázky, videa nebo prosté soubory. Jednotlivé logické celky dat je možné ukládat a organizovat pomocí kontejnerů v rámci úložiště. Blob storage poskytuje několik úrovni přístupu. Od veřejně přístupných dat až po kontrolované a omezené zpřístupněni pomocí klíčů nebo podpisů. Blob storage je robustní, škálovatelné globálně dostupné úložiště nestrukturovaných dat.

- Hlavní vlastnosti Blob storage
  - Škálovatelnost. Špičková navržená odolnost s geografickou replikací a možností podle potřeby flexibilně škálovat.
  - Bezpečnost. Ověřování pomocí Azure Active Directory, řízení přístupu na základě role (RBAC), šifrování neaktivních uložených dat a rozšířená ochrana před internetovými útoky.
  - Komplexní správa dat. Komplexní správa životního cyklu, řízení přístupu na základě zásad a neměnné úložiště (WORM). [1]

Pro relační ukládání dat Azure nabízí Azure SQL database. Služba je poskytována na základech známého Microsoft serveru. Poskytuje vysokou dostupnost, možnosti pro škálování a vysokou úroveň bezpečnosti. Azure SQL database podporuje v podstatě celou škálu funkcionalit jako on premise SQL server, navíc nabízí široké možnosti zálohování, replikace dat, škálování a zabezpečení. V případě, že organizace nechce z nějakých důvodů používat Microsft SQL, nabízí Azure i variantu Postgres SQL database. Samozřejmě i nadále mají organizace možnost provozovat si vlastní relační databázi v Azure v rámci pronajatého virtuálního serveru, ale v tom případě je nutné řešit vysokou dostupnost, škálování a zálohování vlastními prostředky.

- Hlavní vlastnosti Azure SQL databáze
  - Plně spravovaný databázový modul automatizuje aktualizace, zřizování a zálohování, umožňuje organizacím soustředit se primárně na vývoj aplikací.
  - Flexibilní bez serverové výpočetní prostředí s rychlou odezvou a úložiště Hyperscale se rychle umí přizpůsobit aktuálním požadavkům organizace.
  - Integrovaná umělá inteligence a vysoká dostupnost udržují výkon a odolnost ve špičce díky smlouvě SLA zaručující až 99,995% dostupnost. [1]

Zástupcem řešení persistence dat v no SQL databázích je Cosmos DB, jedná se o distribuovanou databázovou službu, která je navržena pro nasazení a škálování globálně distribuovaných aplikací v cloudu. Cosmos DB umožňuje multimodelový přistup. Podporuje dokumentové, grafické, klíč - hodnota a sloupcové databázové modely. Mezi její vlastnosti patři nízká latence, škálovatelnost a globální přistup k datům. Cosmos DB podporuje také API přístup pro MongoDB, Cassandra, Gremlin a Tabulkovou databázi Azure.

- Hlavní vlastnosti Cosmos DB

  - Dobrá výkonnost v jakémkoli měřítku s okamžitou a neomezenou elasticitou, ´podpora rychlého čtení a zápisu ve více oblastech kdekoli na světě.
  - Rychlý a flexibilní vývoj aplikací s bezplatnými možnostmi vývoje a testování, několika sadami SDK a podporou opensourcových databází PostgreSQL, MongoDB a Apache Cassandra.
  - Připravenost pro kritické aplikace s dostupností 99,999 %, nepřetržitým zálohováním a zabezpečením [1]

Poslední zmíněnou možností datové persistence je Azure Data Lake storage. Jedná se o vysoce abstraktní datovou službu, která je vysoce škálovatelná, výkonná a uzpůsobená na ukládání a analýzu velkých objemů dat. Data Lake storage nemá pevně dané schéma a jde tedy o velmi flexibilní úložiště. Umožňuje ukládat libovolné datové ´formáty souborů a podporuje rozšířený souborový systém Hadoop Distributed File System.

- Hlavní vlastnosti Azure Data Lake Storage
  - Škálování bez limitů a automatická georeplikace.
  - Vysoce bezpečné úložiště s flexibilním mechanismem pro ochranu dat komplexně od přístupových práv, šifrování až po kontrolu na úrovni sítě.
  - Nezávisle škálovaní datové a analytické častí, na úrovni objektů a správou životního cyklu dat a vede k zajímavým cenovým optimalizacím[1]

Organizace z případové studie potřebuje ukládat data do relačních databází, dále datové soubory a pro svoji zákaznickou aplikaci potřebuje noSQL databázi MongoDB a timeseries databázi. SLQ databázi potřebují CRM, ERP, portál společnosti a obě zákaznické aplikace. V Azure je několik možností jak relační databázi řešit. První je provozovat SQL server na virtuálním serveru v režimu IaaS. Organizace má tak server plně pod kontrolou, ale zodpovídá si za kompletní administraci, bezpečnost. zálohování a update nejenom databáze, ale i operačního systému serveru.To sebou přináší vetší nároky na provozní tým, který se musí zabývat běžnou operativní činností. Ta, ačkoliv důležitá, je vetšinou rutinní záležitostí a sestává se z mnoha opakujících se kroků. Vyškolení odborníci musí řešit tyto kroky místo aby věnovali čas například inovacím a rozvoji.

Tato nevýhoda odpadá v režimu PaaS Azure nabízí spravovanou službu Azure SQL databáze. Tato služba je postavena na základech Microsoft SQL serveru, je plně spravována poskytovatelem a organizaci tak odpadají starosti s běžnou operativní činností. Poskytovatel se postará o bezpečnost, zálohování a pravidelný update systému.

V naší případové studii volíme variantu Azure SQL databaze, tato služba organizaci umožňuje vytvořit pod jednou administrací několik nezávislých databází. Pro každou aplikaci jedna. Databáze budou mít řízení přístupových práv na základě Azure Active Directory. Databáze budou sdruženy do tzv Elastic poolu.

"Jedná se o jednoduché cenově efektivní řešení pro správu více databází, které mají různé a nepředvídatelné nároky na potřebný výpočetní výkon. Databáze v Elastic poolu jsou na jednom serveru a sdílejí soubor zdrojů za jednu cenu. Elastic pool přináší organizacím řešení software as a service (SaaS) a umožňuje optimalizovat cenu a výkon pro skupinu databází za definovaný budget a přináší tak elastický výkon pro všechny databáze. "[1]

Dalším co musí organizace řešit, je ukládaní souborů a jejich sdílení mezi pracovníky firmy. Jako jedna z možností se nabízí využí Blog storage na kterém se vytvoří SMB share a ten je zpřístupnit uživatelům. Jedná se o technologii známou a dlouhou dobu používanou.

Nicméně neřeší například potřebu sdílet soubory vně organizace s lidmi co nemají účet v AAD. V praxi se nakonec stává, že zaměstnanci soubory vystavují různě po internetu a organizace ztrácí kontrolu nad svými daty.

Možností, jak může organizace lépe udržet sdílení dat pod kontrolou je cloudové řešeni O365, konkrétně One drive.

OneDrive je cloudová platforma společnosti Microsoft, která umožňuje uživatelům ukládat, sdílet a synchronizovat svá data a soubory přes internet.

Jednou z hlavních výhod je synchronizace dat. OneDrive automaticky synchronizuje soubory mezi různými zařízeními, což umožňuje uživatelům přístup k nejaktuálnějším verzím svých souborů. Tím se zajišťuje, že změny provedené na jednom zařízení se projeví na všech ostatních zařízeních, na kterých je OneDrive používán. Tato synchronizace přináší pohodlí a efektivitu při práci s dokumenty a umožňuje uživatelům pracovat na svých projektech kdykoli a kdekoli.

Další výhodou je možnost sdílet soubory a složky s ostatními uživateli. Uživatelé mohou nastavovat oprávnění přístupu a spolupracovat na dokumentech v reálném čase. To je užitečné při spolupráci na projektech s týmem nebo při sdílení souborů s klienty, či externími partnery.

Bezpečnost je také důležitým aspektem OneDrive. Data jsou chráněna šifrováním a uživatelé mají možnost nastavit různá bezpečnostní opatření, jako je dvoufaktorové ověřování, aby se zabezpečily jejich účty a soubory.

Vzhledem k těmto výhodám je OneDrive volbou pro případovou studii v této práci. Poskytuje organizaci pohodlné a efektivní prostředí pro práci s dokumenty a soubory a umožňuje spolupráci.

Poslední otázkou, kterou musí případová studie vyřešit, je noSQL databáze MongoDB a proprietární timeseries databáze. Je samozřejmě možné tyto databáze provozovat v rámci virtuálního serveru, ale znamená to výše zmíněné nevýhody. Azure nabízí databázové řešeni CosmosDB. Jedná se o globálně distribuované řešení, které podporuje multimodelový přístup. Jedním z podporovaných přístupů je API MongoDB. On premise databáze MongoDB dá se nahradit cloudovou databázovou službou CosmosDB s možnosti přístupu jako k MOngoDB.

Z povahy obchodní činnosti organizace vyplývá ještě potřeba nějaké timeseries databáze. On premise řešení bylo proprietární a poskytované tvůrcem zákaznické aplikace. Organizace prodává zařízení s PLC logikou určená k řízeni různých technických zařízeni po celém světě. Zmíněná databáze slouží k ukládání událostí z těchto jednotek.

Možné cloudové řešení v Azure je InfluxDB, jedná se o službu postavenou na open source řešení Influx poskytované Azure. Jednou z klíčových vlastností InfluxDB je jeho schopnost zpracovávat velké objemy časových řadových dat s vysokou rychlostí zápisu a čtení. Databáze je optimalizována pro efektivní ukládání a dotazování časových štítků, což umožňuje rychlé získávání dat z různých zdrojů a jejich analyzování v reálném čase. Tímto způsobem může InfluxDB podporovat různé scénáře, jako je sledování výkonu, sběr dat ze senzorů, logování událostí a mnoho dalších.[16]

V případové studii volíme pro organizaci následující řešení:

SQL databáze budou přesunuty na službu Azure SQL database v režimu Elastic pool. Pro ukládání souborů a jejich sdílení mezi pracovníky i externisty bude nasazeno řešení OneDrive. Organizace dále potřebuje noSQL databázi MongoDB a timeseries databázi, která je v on premise proprietární. MongoDB bude v Azure nahrazeno řešením CosmosDB a bude využito MongoDB model pro přistup k datům přes API. Timeseries databáze bude nahrazena službou InfluxDB Cloud.

7.2.4 Vnitřní sítě

Interní sítě jsou v Azure postaveny na Virtuálních sítích. Jde o privátní virtuální sítě, ve kterých si organizace muže definovat vlastní síťové rozsahy a segmenty a řídit přistup do nich. Sítě jsou vzájemně izolované a fungují v podstatě stejně, jako vlastní datacentrum. Prostředky v cloudu se jednoduše připojují do těchto sítí a tím je zajištěna jejich komunikace. Pomoci Virtuálních sítí je možné vytvářet i složité topologie a oddělovat jednotlivé segmenty sítě. To organizacím mimo Jiné pomáhá udržet lepší přehled v infrastruktuře a rozdělení sítě na jednotlivé segmenty zlepšuje i zabezpečení. V případě úspěšného napadení prostředku z jednoho síťového segmentu, není automaticky útočníkovi zajištěn přistup i do ostatních částí sítě.

K propojeni jednotlivích virtuálních sítí slouží Peering sítě (Virtual netvork Peering) Tato služba umožňuje organizaci spojit dvě nezávislé virtuální sítě v jednu. Komunikace pak probíhá po privátních páteřních spojích společnosti Microsoft a je neveřejná. Umožní tedy komunikaci prostředků z jedné virtuální sítě s prostředky v druhé s nízkou latencí a bez nutnosti použití internetové sítě. Řízení přístupu mezi jednotlivými virtuálními sítěmi je realizováno pomocí síťových skupin zabezpečení, kde je možné podrobně definovat jaké prostředky mají přistup do jakých sítí.

Dále Azure nabízí službu síťové brány, která poskytuje možnosti propojení mezi virtuálními sítěmi v Azure a vaší lokální sítí. Organizace může použít síťovou bránu "VPN Gateway"a vytvořit zabezpečený šifrovaný tunel přes internet, nebo využít síťovou bránu ExpressRoute Gateway, kdy se jedná o ryze privátní propojení síťové infrastruktury organizace a příslušným datacentrem Azure. Expressroute je realizována ve spolupráci s příslušným poskytovatelem konektivity a není nijak vázána na veřejný internet, Jedná se o čistě privátní síť mezi organizací a cloudem Azure, vyznačuje se větší spolehlivostí, vyšší rychlostí, konzistentní latencí a vyšším zabezpečením, než je typické pro řešení spojení organizace s cloudem Azure pomocí veřejného internetu. [16]

Další možností, jak propojit virtuální sítě a lokální síť organizace je služba Azure Virtual WAN. Jediná služba, která umožňuje správu propojení mezi lokalitami v rámci Azure i mimo něj. Pomocí Azure Virtual WAN můžete snadno propojit virtuální síť v Azure s vašimi lokálními sítěmi a vytvořit tak rozsáhlou a centralizovanou síťovou infrastrukturu. V podstatě umožňuje spojit do jedné sítě různé části infrastruktury organizace využívající různé technologie připojení do cloudu Azure. Například může jít o geograficky odloučené pobočky, a virtuální sítě v Azure. Služba podporuje různé druhy připojení jako je site to site a pint to site VPN, SD-WAN, Express route, připojení v rámci cloudu a další.

"Azure virtual WAN se tak stane jednotnou platformou pro správu a řízení síťových připojení organizace. Navíc poskytuje potenciál pro rozvoj i do budoucna."[16]

Virtuální sítě v Azure je ještě možné zabezpečit službou Azure Firewall, která poskytuje centrální zabezpečení a správu pro virtuální sítě v Azure. Můžete ho použít k ochraně a monitorování provozu mezi virtuálními sítěmi v Azure a vaší lokální sítí. Jedná se o výkonný, neomezeně škálovatelný firewall s vysokou dostupností.

"Microsoft investuje do výzkumu a vývoje v oblasti kybernetického zabezpečení více než 1 miliardu USD ročně. A zaměstnává více než 3 500 odborníků na zabezpečení, kteří se plně věnují zabezpečení dat a ochraně osobních údajů."[16]

Všechny tyto možnosti umožňují organizaci propojit vnitřní síť v Azure s vlastní lokální sítí v kancelářích a poskytují různé způsoby a úrovně zabezpečení. Volba závisí na vašich konkrétních potřebách a požadavcích na síťovou infrastrukturu.

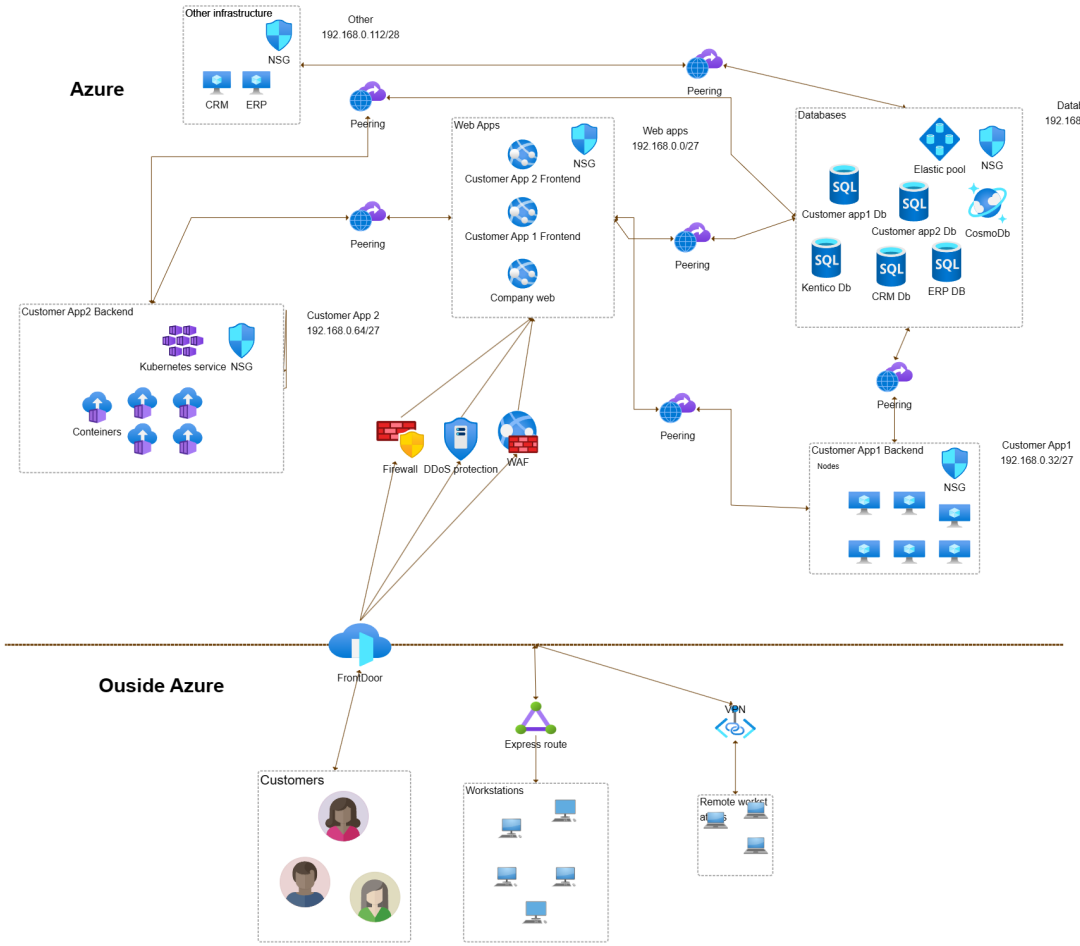
Pro případovou studii bude pro organizaci síťové propojení řešeno následovně. V Azure budou vytvořeny následující virtuální sítě.

Tabulka 7: Virtuální sítě

Název	Rozsah	Počet adres
Web Apps	192.168.0.0/27	32
Databases	192.168.0.96/28	16
Other	192.168.0.112/28	16
Customer app1	192.168.0.32/27	32
Customer app2	192.168.0.64/27	32

Potřebná propojení mezi virtuálními sítěmi bude realizováno peeringem, kdy bude komunikace povolena pouze na definované porty a IP adresy.

Propojení se sítí organizace bude realizováno bránou VPN u všech poboček. Globálně bude síť spravována pomocí služby Azure WAN a zabezpečena službou Azure Firewall.



Obrázek 7: Segmentace sítě

7.2.5 Bezpečnost a stabilita

Cloudové řešeni společnosti Microsoft disponuje mnoha nástroji a řešeními, které podporují bezpečnost aplikací a infrastruktury provozované v Azure. V této části se práce zaměří na vybrané klíčové oblasti.

Jako první je třeba řešit identitu a řízeni přístupu uživatelů. V Azure je toto řešeno službou Azure Active Directory. Tato služba poskytuje centrální správu uživatelů, jejich rolí a identit. Podporuje dvoufaktorovou autentizaci a jedno přihlášení (Single sign on). Je možné ji integrovat i s on premise Active Directory serverem a používat stejné účty jak pro Azure, tak i například pro pracovní stanice uživatelů. Rozšířením této služby je Azure Active Directory B2C, která slouží k řízení identit a rolí zákazníků organizace. Poskytuje stejné možnosti i zákazníkům, jako je dvoufaktorová autentizace nebo jedno přihlášení, ale zákazníci jsou bezpečně izolováni a mohou se přihlašovat pouze do aplikací, které jsou integrovány pomocí protokolu OAUTH2 a JWT tokenů nebo OpenID connect či SAML protokolů.

Další oblastí je síťová bezpečnost. Azure disponuje mnoha možnostmi, jak ji zajistit. Už při designu sítě nabízí možnosti využití virtuálních sítí a tak izolovat jednotlivé segmenty sítě, následně pomocí síťových zásad nastavit pouze povolený provoz mezi nimi.

Dalšími prostředky jsou Azure Firewall, Azure DDoS ochrana, a samozřejmě monitoring například službou Azure Insights nebo službou Microsoft Sentinel.

"Microsoft Sentinel je služba SIEM (Security Information and Event Management), která využívá umělou inteligenci. Tato služba poskytuje proaktivní detekci hrozeb, prověřování a reakce, což umožňuje odhalování sofistikovaných hrozeb a následné účinné reakce na ně."[1]

Je také podporováno šifrování dat. A to jak dat v klidu, tak i dat na cestě. Pomocí služby Azure Disk Encryption lze šifrovat uložená data a při přenosu dat lze využít zabezpečeného přenosu protokolem DevOps nebo využít Azure VPN pro zabezpečené spojení mezi lokalitami za použití nejmodernějších šifrovacích algoritmů.

Azure také nabízí různé možnosti zálohování, replikace a obnovy dat. Pomocí služby Azure backup je možné centralizovat zálohovaní dat, je podporována záloha jak v rámci lokality, tedy jednoho datacentra, tak i geograficky oddělené zálohování do jiných datacenter. V případě, že obnova ze zálohy by trvala příliš dlouho a ohrožovala bussines organizace, je možné využít služby replikace dat, která je také možná lokálně, nebo do jiného datacentra.

Zajímavým řešením v Azure je služba Azure Key Vault, kde je možné ukládat certifikáty a aplikační hesla, která nejsou nadále nikde přístupná. V případě potřeby je k příslušnému heslu přistup umožněn pouze pomocí klíče svázaného se spravovanou identitou. Jiné metody přístupu, jako je instantní objekt a klíč, nebo hlavní objekt služby a klíč se nedoporučují s ohledem na bezpečnost nebo náročnost použití. Klíče a certifikáty mohou být uloženy v hardwarových modulech.

Azure také dodržuje různé mezinárodní standardy bezpečnosti a je držitelem certifikací, jako je ISO 27001, SOC 1 a SOC 2.

Pro potřeby případové studie bude bezpečnost v Azure řešena následovně. Prostředí bude síťově rozděleno na logické segmenty s vlastním rozsahem IP adres. Komunikace mezi nimi bude omezena na nezbytné minimum, a bude nasazen Virtual network peering. Tím bude zajištěna komunikace pouze po neveřejné sítí Microsoftu. Pomocí skupin síťových zabezpečení budou povoleny pouze nezbytné porty a IP adresy.

Veřejný přistup z internetu bude realizován službou Azure FronDoor ve které bude zařazen firewall, DDoS ochrana a terminace šifrovaných spojení. Všechny šifrovací certifikáty budou uloženy ve službě Azure Key Vault, stejně jako hesla a klíče aplikací.

Všechna data budou šifrována na úložištích. Bude nasazena služba Azure Backup ve dvou úrovních. Nejdůležitější data budou zálohována do geograficky oddělených datacenter, méně důležitá data budou zálohována lokálně ve stejném datacentru.

Všechny prostředky budou logovat do služby Azure Insight a logy budou vyhodnocovány službou Microsoft Sentinel.

7.3 Správa a optimalizace cloudového prostředí

Azure ze své podstaty nabízí mnoho možností pro správu a optimalizaci infrastruktury. Patří sem správa zdrojů, monitorování výkonu, škálování a správa nákladů.Tato část diplomové práce poskytne přehled o klíčových oblastech, které je třeba zvážit a implementovat při používání Azure pro efektivní správu a optimalizaci výkonu.

Jako první se práce zaměří na správu zdrojů v Azure. Nejvýše v hierarchii infrastruktury stoji "tenant".

"Tenant je instance Služby Azure Active Directory (Azure AD), ve které se nacházejí informace o jedné organizaci, včetně organizačních objektů, jako jsou uživatelé, skupiny a zařízení, a také registrace aplikací, jako je Microsoft 365 a aplikace třetích stran."[1]

Tenant tedy zahrnuje pod sebou všechny prostředky organizace do jednoho logického celku. Organizace samozřejmé může mít více tenantů, ale jedná se o poměrně izolované celky a stejně jako v on premise, je pro vzájemné přístupy na prostředky nutné navazovat obdobou doménových vztahů důvěry.

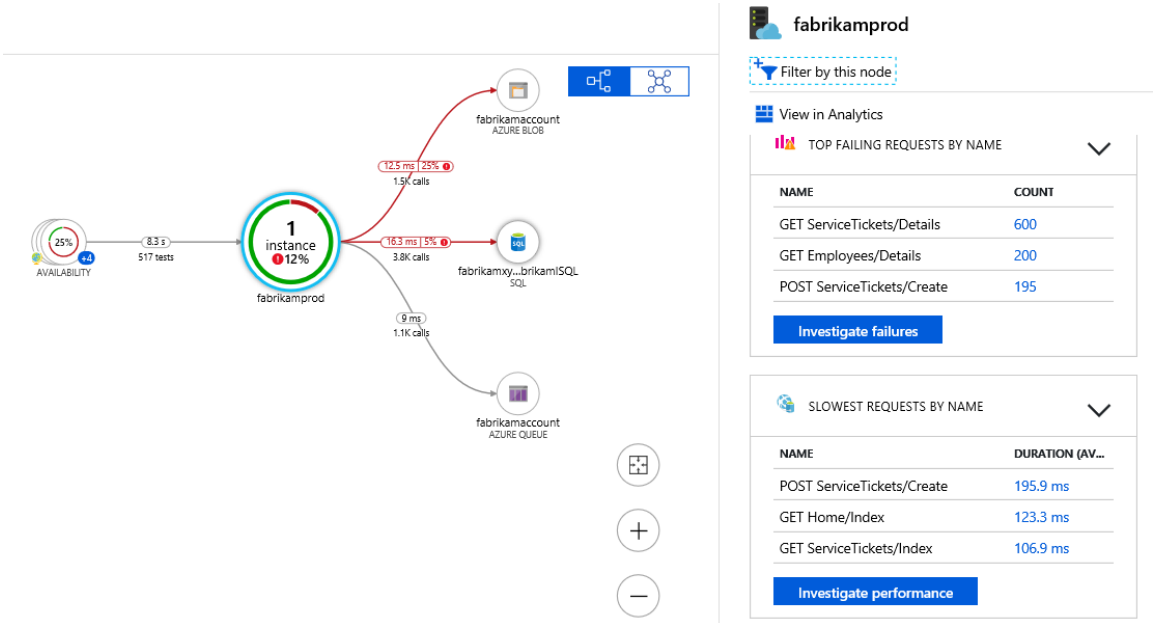
Pod tenatem je možné rozdělit infrastrukturu na skupiny zdrojů (Resurce Groups). Jedná se o kontejnery, které obsahují skupiny prostředků pro nějaké řešení. Skupina prostředků může obsahovat všechny prostředky se vztahem k určitému řešení, nebo jenom některé. Je na uvážení organizace, jak si prostředky do skupin prostředků rozdělí. Obecně je lepši sdružovat do skupin prostředky se stejným životním cyklem, což vede k zjednodušení správy a řízení přístupu k těmto prostředkům. Dále je možné skupiny prostředků využít k rozdělení na testovací a produkční prostředí. Skupiny prostředků se navzájem nijak neovlivňují a je tak zajištěna izolace testovacího a produkčního prostředí.

Ke správě prostředků je možné také využít službu Azure resource manager. Jedná se o nástroj, který umožní organizaci automatizaci správy zdrojů pomocí šablon. Jedná se o šablony ve formátu JSON, ve kterých je možné definovat jaké prostředky a s jakými uživatelskými přístupy se mají vytvořit. Azure resource manager pak zařídí jejich vytvoření a nasazení. Tento proces může být součásti pipeline a plně tak automatizovat nasazování aplikací v Azure.

Součástí správy prostředí, která často vede k optimalizaci, je i kvalitní monitoring zdrojů. Azure nabízí možnost využívat monitorovací službu Azure Insight a Log Analytics. Obě tyto služby slouží ke sběru logu a událostí. Azure Insights sbírá a vyhodnocuje stavy v reálném čase. Má mnoho před připravených dashboardů a metrik, které je možné sledovat a při definovaných stavech upozornit pomocí alertu zodpovědného pracovníka. Jedná se například o vytížení CPU, Paměti, počtu reqestů úspěšných a neúspěšných. Každý prostředek v Azure disponuje sadou relevantních metrik v Azure Insigts. Log Analitics je určen k podrobnější analýze logů. Pomáhá při hledání souvislostí a vztahů mezi událostmi.

Azure dále disponuje možností vytvářet si uživatelsky definované dashboardy. Organizace si tak může vytvářet dashboardy na míru pouze s relevantními metrikami.

poslední možností monitoringu zmíněné v této práci je možnost generování aplikačních map. Na takových mapách je možné sledovat stav prostředků konkrétní aplikace, vazeb uvnitř a celkové kondice služby. Ukázka takové mapy je na následujícím obrázku 8.



Obrázek 8: Aplikační mapa ukázka[1]

Optimalizace provozu se také týká škálování. Škálovat se dá buď horizontálně, tedy přidáváním dalších prostředků se stejnou funkcí, které se o zátěž podělí. Zde musí být ale běžící aplikace na takové fungování připravena. Například webové stránky a vyřešený session state. Další možností je škálovat vertikálně, tedy přidávat výkon pomocí CPU, paměti či disků. Takto se dají škálovat například virtuální servery, databáze, Kubernetes clustery atd. Většinou to znamená, že se na pozadí vytvoří kopie prostředku a po synchronizaci je na něj převeden provoz. Z podstaty to většinou znamená škálování s výpadkem.

Většina prostředku u kterých to dává smysl je v Azure škálovatelná. Pomocí služby Azure Automation je možné škálovat i automaticky, a to za pomocí trigerru, události nebo dle časového plánu. To má dopad, jak na výkon systému, který je ve správnou dobu k dispozici, tak i na cenovou optimalizaci, kdy je dostupný výkon snižován v době, kdy není potřeba. Tím pádem je organizace schopna vykrývat špičky ve kterých je nutný velký výkon prostředků, aniž by musela investovat do hardware, který není většinu času využit. Nicméně některé prostředky nelze z jejich povahy škálovat bez výpadku a je nutné na tuto okolnost vytváření škálovacích plánů brát ohled.

Také kontrola nákladů je pro organizace důležitým aspektem provozu IT. Azure nabízí možnosti k takové kontrole nástroji pod souhrnným názvem "Azure Cost Management". U každé skupiny služeb je možné sledovat aktuálně utracené prostředky s predikcí do konce měsíce. Náklady lze rozpadnout až na úroveň konkretních prostředků.

Dále je možné nastavit cenové hladiny a v případě, že hrozí jejich dosažení, informovat zodpovědné osoby e-mailem. Nejpřísnější možností jak hlídat náklady, je nastavit nepřekročitelný budget skupiny prostředků. Služby, po dosažení takového limitu jsou následně

zastaveny až do konce zúčtovací periody. To se hodí zejména u testovacích prostředí. Naopak takové nastavení nebude vhodné pro produkční nasazení.

K otázce nákladů patří i možnosti slev, které jsou v Azure možné zejména pro různé předplatné. Pokud organizace dokáže predikovat jaké prostředky přibližně bude v následujícím období potřebovat, je možné je předplatit se slevou v řádech desítek procent.

Pro potřeby případové studie bude prostředí organizace rozděleno do následujících skupin zdrojů.

Tabulka 8: Rozdělení do skupin zdrojů

Skupina zdrojů	Prostředky
Webové aplikace	Company Web app Customer app1 Web app Customer app2 Web app
Databases	SQL Elastic pool SQL databases - ERP, CRM, Customers App1 & 2, Kentico Cosmos Db
Customers App1	Backend virtual servers
Customers App1	Kubernetes cluster
Customers App1 Test	Test virtual servers
Customers App1 Test	Test Kubernetes cluster

bude nakonfigurován application Insigts jako monitoring, vytvořeny provozní dashboardy a aplikační mapy dle požadavku jednotlivých týmů.

Na vývojová a testovací prostředí budou stanoveny nepřekročitelné budgety a náklady produkce budou hlídány pomocí nastavení cenových hladin a upozorněním zodpovědným osobám.

7.4 Vývoj a nasazováni v cloudu

Vzhledem k tomu, že organizace provádí i vlastní i delegovaný vývoj vlastích aplikací či firmware pro výrobky, potřebuje i nástroje pro vývoj. Azure nabízí komplexní škálu nástrojů pro vývoj, testování a nasazování software pod souhrnným názvem Azure DevOps. Vývojovým týmům tato sada nástrojů dokáže značně usnadnit práci. Umožňuje spolupráci na projektech, jejich vedení od zadání až po otestování a nasazení. Součástí DevOps je také mnoho automatizačních nástrojů a vývojářům tak zbývá více prostoru pro samotný vývoj softwaru.

Klíčové složky v Azure DevOps:

- Azure Boards, nástroj pro správu projektů a sledování práce.
- Azure Repos, nástroj pro správu zdrojového kódu.
- Azure Pipelines, nástroj pro automatizaci pro sestavení a nasazení softwaru.
- Azure Test Plans, nástroj pro sledování a řízení testování softwaru.

Azure Boards je nástroj, který poskytuje vývojářům prostředky pro plánování, sledování a spolupráci na různých projektech. Jeho klíčovou funkcí je umožnění organizace úkolů do logických skupin nazvaných Epicy a User Stories, což vytváří hierarchickou strukturu, a umožňuje tak řízeni, sledovaní a organizaci celých projektů.

Dalším nezbytným nástrojem je Azure Repos, verzovací systém založený na technologii GitHub. Vývojářům umožňuje pokročilou správu kódu, jeho verzování a sledování změn. Je podporován většinou známých vývojářských nástrojů, jako je Visual Studio, Eclipse, Net Beans a další. Zajimavá je jeho integrace do Azure Pipelines a tedy možnost plně automatizovat proces sestavení, otestování a nasazení do produkce.

Azure Pipeline je vpodstatě sada kroků, které jsou automaticky či ručně provedeny a na základě jejich stavu je spuštěn či nespuštěn další krok. Jde o systém tzv bran, kdy pipeline buď může, nebo nemůže pokračovat dále. Vyhodnocení stavu může být automatické nebo i ruční. Je tedy možné do logické posloupnosti integrovat kroky jako stažení kódu z repositáře, code rewiew, různé testy jak funkční, tak i bezpečnostní, sestavení na testovací prostředí a nakonec sestavení na produkci. Samozřejmostí je díky verzovacímu systému Azure Repos možnost návratu k předchozím verzím kódu v případě výskytu nějaké závažné chyby.

Každý softwarový projekt by měl mít také definováno, jak bude otestovaná jeho funkčnost. K tomu slouží v DevOps nástroj Azure Test Plans. V něm je možné definovat jednotlivé kroky testů a jaký mají mít výsledky. Tyto je pak možné automatizovat, nebo i testovat ručně. Mohou být integrovány do pipeline a organizace tak, díky systému bran v pipeline, má jistotu, že není nasazen neotestovaný software.

Díky možnostem cloudového řešení je také snadné vytvářet si testovací prostředí. Pro účely případové studie budou vytvořena tři prostředí. První bude určené pro vývoj aplikací, bude k dispozici vývojářům, kteří v něm budou moci svobodně deployovat různé Azure služby určené k testovaní a vývoji. Náklady na toto prostředí budou kontrolovány přidělením maximální povolené částky, kterou je možné měsíčně utratit, tzv. Budgetem.

Dalším prostředím bude prostředí testovací, zde budou pravidla stejná jako na produkci, včetně bezpečnostních omezení. Toto prostředí bude součástí Azure pipelines a bude určené k předprodukčnímu testováni aplikací.

Posledním prostředím bude prostředí produkční. Organizace bude používat nástroje DevOps nejenom pro vývoj, ale i pro provozní část. Zpětná vazba z provozu směrem k vývojářům a řešení závad bude zajištěno pomocí azure Boards. Nástroj Azure Repos zajistí i správu kódu.

7.5 Empirické porovnání výkonu databáze on premise a Azure

Součásti migrace by mělo být i závěrečné vyhodnocení a validace, zda byla migrace přínosná a efektivní. V této práci je provedeno porovnání rychlosti zápisu a čtení různě velkých dat do PostgresSQL databáze ve verzi on premise a v Azure cloudu.

Jako testovací vzorek byla použita tabulka s názvem "customers"Obsahovala následující sloupce:

id INT, first_name VARCHAR(50), last_name VARCHAR(50), e-mail VARCHAR(50), gender VARCHAR(50), cc VARCHAR(50), balance VARCHAR(50), aktivní VARCHAR(50)

Data byla náhodně vygenerována do šesti balíčku po 1,10,100,1000,10000,100000 řádcích. Ty byli postupně zapsány do databáze a následně čteny. Postgres DB byla zvolena ve verzi 15 a hardware byl použit následující.

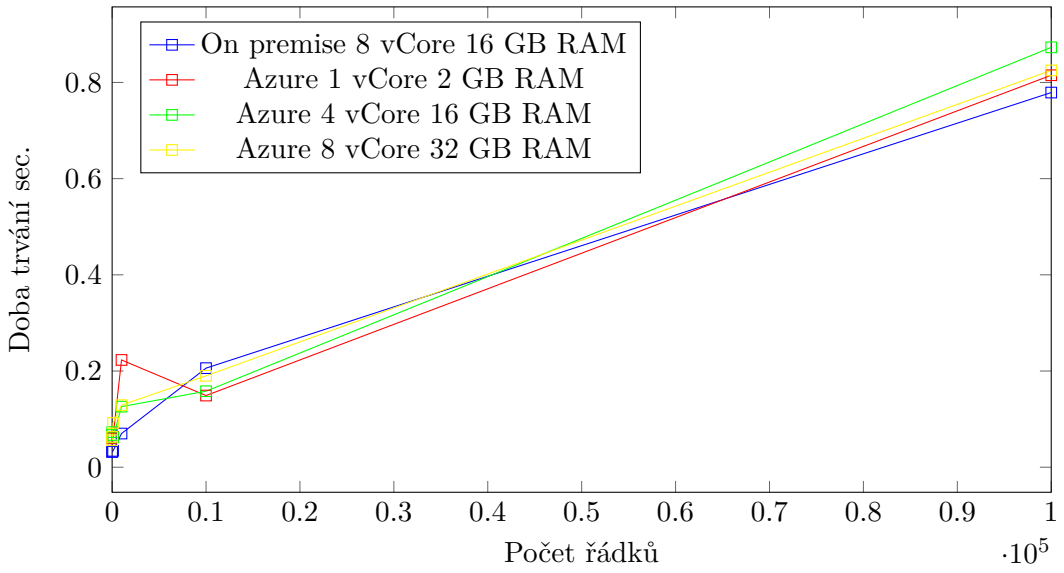
Tabulka 9: Použitý hardware

Varianta	Prostředky
On premise server	8 vCore 16 GB RAM
Azure varianta 1	1 vCore 2 GB RAM
Azure varianta 2	4 vCore 16 GB RAM
Azure varianta 3	8 vCore 32 GB RAM

Výsledky testu jsou uvedeny v následující tabulce grafech.

Tabulka 10: Výsledky měření

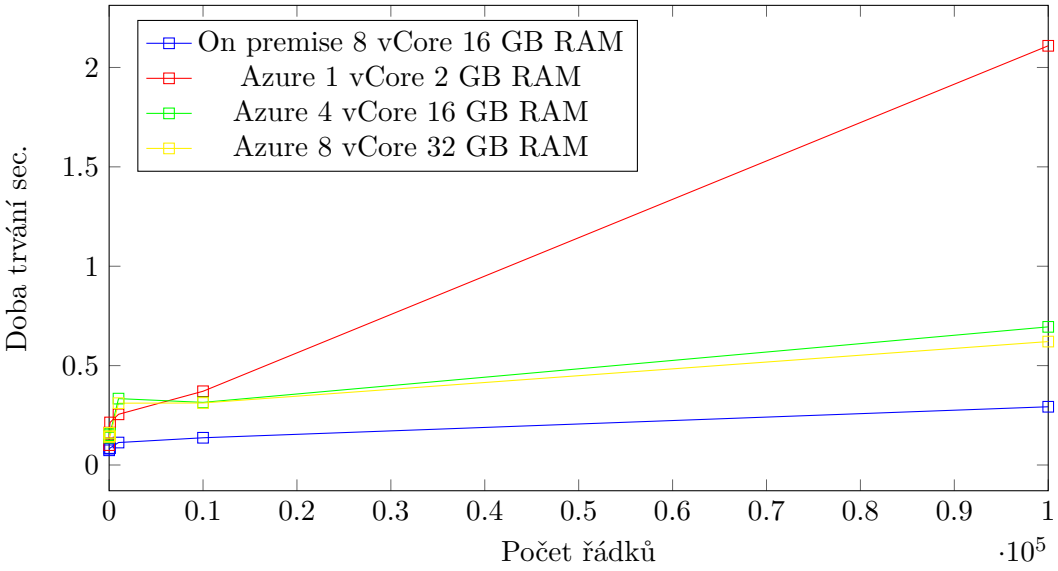
Počet řádku	On Premise	Azure varianta 1	Azure varianta 2	Azure varianta 3
	zápis/čtení	zápis/čtení	zápis/čtení	zápis/čtení
1	0.032/0.074	0.060/0.1	0.067/0.138	0.063/0.162
10	0.032/0.082	0.061/0.163	0.073/0.150	0.056/0.141
100	0.034/0.085	0.063/0.214	0.062/0.159	0.092/0.145
1000	0.070/0.113	0.223/0.255	0.126/0.334	0.129/0.311
10000	0.206/0.137	0.149/0.371	0.158/0.315	0.190/0.695
100000	0.779/0.293	0.815/2.109	0.873/0.312	0.825/0.621



Obrázek 9: Rychlost zápisu dat do PostgeSQL databáze

Z dosažených výsledků je zjištěno, že při přechodu do Azure cloudové služby nedochází k žádnému významnému zhoršení výkonu při zápisu. Pouze ve variantě Azure 1. která byla volena jako nejmenší možná konfigurace v Azure bylo dosaženo horších výsledek než na on premise databázi. Při volbě následující možnosti, tedy 4 vCPU a 16 GB RAM, tedy pořád méně než v on premise řešení, je už dosaženo výsledků srovnatelných s lokální databází. Další škálování hardwaru už významný efekt pro zápis nepřineslo.

Trochu jiná situace byla u čtení dat. Při testu bylo zjištěno, že varianta v Azure vykazuje mírnější zhoršení v časech potřebných pro čtení dat z databáze. U varianty 1 došlo k



Obrázek 10: Rychlost čtení dat z PostgeSQL databáze

výraznému zhoršení a varianty 2 a 3 k méně významnému zhoršení. Zvláštní je situace, kdy při přidání CPU došlo paradoxně ke zhoršení výsledků ve čtení dat.

Je tedy nutné zvážit zda je takové zhoršení pro organizaci přijatelné.

8 Kritické zhodnocení návrhu

V praktické části diplomové práce bylo představeno jedno z mnoha možných řešení migrace organizace z on premise řešení infrastruktury do Azure.

Jako první krok byla provedena konfigurace Azure active directory a její propojeni se stávajícím Active directory organizace. Vzhledem k tomu, že se jedná o nativní řešení Microsoftu, tak veškerá funkcionalita zůstala neměnná. Řízeni uživatelských práv bylo zachováno a rozšířeno o funkcionalitu potřebnou pro cloud Azure. Organizace navíc získala možnost používat službu Azure active directory B2C, která slouží k pokročilému řízení přístupu zákazníků k aplikacím společnosti s vysokým zabezpečením, jako je například multifaktorové ověřovaní.

Běžné služby, jako je e-mailovy server, Teams komunikace a sdílení souborů bylo převedeno na službu SaaS, tedy se o provoz aplikace stará kompletně poskytovatel služby, v našem případě společnost Microsoft a organizace řeší pouze konfiguraci. Spolu s mailovým řešením O365 organizace zároveň vyřešila problematiku kancelářské aplikace MS Office, která je a součásti služby a každý uživatel má k dispozici kompletní sadu nástrojů Office. Vzhledem k tomu, že organizace používá jako ERP a CRM systém aplikace postavené na platformě MS Dynamics, byla také zvolena varianta SaaS MS Dynamics 365.

Vlastní aplikace vyvíjené organizací byly převedeny na platformní služby PaaS. Zejména na web apps a AKS kontejnery. Zde organizace musela dbát na zvolení správného sizingu služby a testování, aby nedošlo k problémům a dopadům na zákazníky, kteří jsou na nedostupnost služby citlivý. Nicméně jednou z předností cloudových služeb, je možnost snadného a rychlého škálování. V případě nenadále potřeby je tedy možno problémy s výkonem rychle a snadno řešit.

Spolu s přechodem do Azure organizace také získala možnost pokročilého monitoringu a analýzy logů. To usnadňuje administrátorům správu a provoz systému a má pozitivní vliv na celkovou stabilitu aplikací.

Za zmínku také stojí zvýšená míra bezpečnosti a ochrany aplikací, která je v Azure na vysoké úrovní a je poskytováno mnoho nástrojů na její řízení. Organizace tak získala možnost využívat bezpečnostní řešeni, které je vyvíjeno a zdokonalováno společností Microsoft, která má díky velkému množství uživatelů a tak i vzorků chování systémů možnosti jak své systémy učit správně reagovat. A díky samotným výpočetním možnostem cloudu Azure na otázky bezpečnosti aplikovat i řešení pomocí umělé inteligence.

Samotná realizace migrace byla poměrně bezproblémová. Azure má velmi dobře zpracovanou dokumentaci a je k dispozici obrovské množství tutoriálu a ukázek, jak běžné konfigurace řešit. Během migrace bylo také ověřeno, že podpora ze strany Microsoftu pro Azure je na velmi dobré úrovni a funguje spolehlivě. Dále existuje mnoho jak on-line tak off line školení, která je možné zakončit i certifikací. Je tedy možné nechat příslušné pracovníky i profesionálně vyškolit.

Objektivně je nutno také říci, že při přechodu do Azure se organizace musela vyrovnat i s několika problémy. Obecně je to nedůvěra zaměstnanců, ale i managementu v nové technologie, dále nutnost doplnění schopností nejenom administrátoru ale i běžných uživatelů. Dále bylo testy zjištěno, že služba SQL serveru v Azure podává lehce horší výsledky při čtení dat z databáze v Azure. Nicméně bylo rozhodnuto, že toto zhoršení nemá významný dopad a není nutné kvůli němu migraci zrušit,

9 Závěry a doporučení

Cílem diplomové práce bylo poskytnout komplexní přehled o možnostech procesu migrace on premise infrastruktury do Microsoft Azure. Dále navrhnout možný postup jak takovou migraci v organizaci realizovat.

Proto byly v teoretické částí představeny hlavní výhody a nevýhody cloudového řešení, dále nastíněny možnosti a zjednodušený proces, jak problematiku řešit a úspěšně migrovat on premise systémy do cloudového řešení.

V práci jsou identifikovány jak silné, tak i slabé stránky takového řešení. Cloudová ´řešení jsou citlivá na kvalitu a spolehlivost internetového připojení. Organizace musí zajistit potřebnou kvalitu připojení a mít i náhradní plán, kdyby došlo s delšímu výpadku konektivity. Dále musí věnovat pozornost i právním otázkám, zejména kvůli nakládáni s daty a v neposlední řadě se organizace vystavuje riziku Vendor lock-in situaci, kdy se může stát plně závislou na jednom dodavateli služeb.

Na druhou stranu v cloudu získává organizace možnosti technologických inovací, které bývají v on premise vždy nákladné a pracné, dále možnosti jak efektivněji řídit náklady a platit pouze za takový výkon a služby, který je aktuálně potřeba. Velkým přínosem je pak omezení rutinní práce administrátorů a potenciál jejich využití k inovacím a realizaci nových projektů a nápadů.

V práci byl dále proveden přibližný výpočet a srovnání nákladů na řešení on premise a Azure cloud pomocí nástroje TCO kalkulátor společnosti Microsoft. Byla zjištěna možná úspora nakladu na provoz IT služeb ve výši 705 458 Eur během pěti let. Z pohledu efektivity tedy případná migrace služeb nabízí minimálně možnosti k finančním úsporám.

V Provedené případová studii bylo hledáno řešení migrace středně velkého podniku s jeho aplikacemi do cloudového prostředí. Byl navržen postup kroků i přibližný časový harmonogram pomocí Ganttova diagramu. Byla nalezena jak řešení běžné komunikace zaměstnanců jako jsou e-maily, instant messaging a sdílení souborů, kdy bylo zvoleno řešení SaaS, tedy plně přeneseni starosti o tyto systémy na cloudového poskytovatele. Dále byly řešeny informační systémy, jako je ERP a CRM, kde byla zvolena opět cesta SaaS, pokud je taková v Azure nabízena. V opačném případe je vždy možnost využit virtuální server.

Jako poslední byly řešeny zákaznické aplikace, které byli přeneseny do platformních služeb v režimu PaaS. Tedy platformní PostgreSQL server, Influx DB, Cosmos DB a web apps.

Vzhledem k tomu, že organizace provádí i vlastní vývoj software je dalším přínosem přechodu do cloudu Azure zavedení procesů DevOps. Azure má užitečný nástroj Azure DevOps, který významně pomáhá takové procesy zavést a udržovat.

Cloudové řešení také přineslo pokročilé možnosti monitoringu a analýz provozu či logů, jak z provozního, tak i z bezpečnostního pohledu. A samozřejmé možnosti škálovat infrastrukturu dle aktuálního provozu a potřeb organizace.

Nicméně pro hladký přechod do Azure je také třeba aby organizace nepodcenili plánování zejména odbornou přípravu příslušných zaměstnanců. Je zde reálné nebezpečí zvýšených, nebo dodatečných nákladů a nebo i neúspěšné migrace. Dalším rizikem je možnost Vendor lock in. Ačkoliv je společnost Microsoft, ale i ostatní velcí poskytovatelé cloudových služeb seriózními partnery, tak toto nebezpečí existuje a může do budoucna přinášet problémy. Otázkou vendor lock in by měla organizace zvážit a vyhodnotit rizika.

10 Budoucí možnosti výzkumu

Řešení společnosti Microsoft Azure, ale i jiní poskytovatelé cloudovych služeb nabízejí služby, které by se mohly považovat za jisté přiblížení se k umělé inteligenci. Microsoft azure například nabízí funkce sdružené pod obchodním názvem Azure AI Services. Nabízejí možnost analyzovat například fotografie, videa. Jazykové modely Azure Open AI pro analýzu a práci s textem. Dále Machine learning a další. Obor umělé inteligence se bouřlivě rozvíjí a další možnosti budou jistě přibývat. Dalším aspektem je dostupný výpočetní výkon, který by v on premise byl prakticky nedosažitelný.

Dostupný výpočetní výkon, funkce umělé inteligence a statistické nástroje dávají mnoho prostoru, jak využít tyto možnosti v provozu a správě IT organizací. Například v analýze logů, bezpečnosti, prediktivním monitoringu a předpovědích selhání. Všechny tyto možnosti je vhodné v budoucnu prozkoumat a hledat jejich praktické využití.

Literatura

[1] Microsoft. Dokumentace k Azure. Available from: https://learn.microsoft.com/cs-cz/azure/?product=popular

[2] Suryawan, R. B.; Ferdiana, R.; Widyawan. The Comparison of Cloud Migration Effort on Platform as a Service. volume 1577, no. 1: p. 012056, ISSN 1742-6588, 1742-6596, doi:10.1088/1742-6596/1577/1/012056. Available from: https://iopscience.iop.org/article/10.1088/1742-6596/1577/1/012056

[3] Costa, P. J. P. d.; Cruz, A. M. R. d. Migration to Windows Azure – Analysis and Comparison. volume 5: pp. 93–102, ISSN 22120173, doi:10.1016/j.protcy.2012.09.011. Available from: https://linkinghub.elsevier.com/retrieve/pii/S2212017312004422

[4] Tran, V.; Keung, J.; Liu, A.; et al. Application migration to cloud: a taxonomy of critical factors. In *Proceedings of the 2nd International Workshop on Software Engineering for Cloud Computing*, ACM, ISBN 978-1-4503-0582-2, pp. 22–28, doi:10.1145/1985500.1985505. Available from: https://dl.acm.org/doi/10.1145/1985500.1985505

[5] Gholami, M. F.; Daneshgar, F.; Beydoun, G.; et al. Challenges in migrating legacy software systems to the cloud — an empirical study. volume 67: pp. 100–113, ISSN 03064379, doi:10.1016/j.is.2017.03.008. Available from: https://linkinghub.elsevier.com/retrieve/pii/S0306437917301564

[6] Rai, R.; Sahoo, G.; Mehfuz, S. Advancements and approaches towards moving from legacy application to cloud. volume 16, no. 2: p. 114, ISSN 1754-3916, 1754-3924, doi:10.1504/IJCNDS.2016.074547. Available from: http://www.inderscience.com/link.php?id=74547

[7] Johnson, L.; Callaghan, C.; Balasubramanian, M.; et al. Cost Comparison of an On-Premise IT Solution with a Cloud-Based Solution for Electronic Health Records in a Dental School Clinic. volume 83, no. 8: pp. 895–903, ISSN 00220337, doi:10.21815/JDE.019.089. Available from: http://doi.wiley.com/10.21815/JDE.019.089

[8] Hazdun, N. Council Post: Cloud Versus On Premises: Advantages And Disadvantages Of Both Models. Available from: https://www.forbes.com/sites/forbestechcouncil/2023/03/27/cloud-versus-on-premises-advantages-and-disadvantages-of-both-models/

[9] What are the biggest disadvantages of cloud computing? | Gartner Peer Community. Available from: https://www.gartner.com/peer-community/poll/biggest-disadvantages-cloud-computing

[10] Gartner: changes in WAN requirements, SD-WAN/SASE assumptions and magic quadrant for network services – Technology Blog. Available from: https://techblog.comsoc.org/2023/03/14/gartner-changes-in-wan-requirements-sd-wan-sase-assumptions-and-magic-quadrant-for-network-services/

[11] Mgr. Bohuslav Lichnovský, LL.M., Mgr. František Nonnemann. Cloudy a právo - 1 díl: Proč o nich uvažovat a n. Available from: https://www.epravo.cz/top/clanky/cloudy-a-pravo-1-dil-proc-o-nich-uvazovat-a-na-co-se-pripravit-115077.html

[12] Leoš Karásek. Technická opatření pro plnění GDPR. Available from: https://theses.cz/id/p3hjy6/

[13] Katie Terrell Hanna. What is vendor lock-in? | Definition from TechTarget. Available from: https://www.techtarget.com/searchdatacenter/definition/vendor-lock-in

[14] Grasseová, M.; Dubec, R.; Řehák, D. *Analýza podniku v rukou manažera: 33 nejpoužívanějších metod strategického řízení*. BizBooks, second edition, ISBN 978-80-265-0032-2, OCLC: 817048500.

[15] Zhou, L. CloudFTP: A Case Study of Migrating Traditional Applications to the Cloud. In *2013 Third International Conference on Intelligent System Design and Engineering Applications*, IEEE, ISBN 978-1-4673-4893-5 978-0-7695-4923-1, pp. 436–440, doi:10.1109/ISDEA.2012.108. Available from: http://ieeexplore.ieee.org/document/6456653/

[16] Microsoft. Azure. Available from: https://azure.microsoft.com/cs-cz/

[17] OWASP. OWASP.org. Available from: https://owasp.org/www-community/attacks/Denial_of_Service

Seznam zkratek

CRM Customers relatioship management - Nástroj řízeni vztahů se zákazníky

DDoS Distributed denial of service - distribuované odepření služby.

DevOps Development and Operations

ERP Enterprice resource plannig - Nástroj pro plánováni zdrojů

IaaS Infrastructure as a service - Hardware poskytovaný jako služba

IaC Infrastructure as Code - Definování infrastruktury pomocí kódu

IT Information technologies - Informační technologie

MD Man day's - Jednotka práce odvedené jedním člověkem za den.

NAT Network address translation - překlad síťových adres.

PaaS Platform as a service - Platfroma poskytovaná jako služba

PLC Programmable logic controller - programovatelný logický automat.

QoS Quality of services - smluvně zaručená kvalita služeb.

RPO Recovery point objective - Časový bod ze kterého je možné obnovit zálohu

RTO Recovery time objective - Čas potřebý k obnově ze zálohy

SaaS Software as a service - Aplikace poskytovaná jako služba

SD-WAN Software defined wide area network - Softwarové definovaná rozlehlá síť

SLA Service level agreement - smluvně zaručena úroveň služby.

TCO Total cost of ownership - Celkové naklady na provoz a vlastnictví

VPN Virtual private enetwork - virtuální privátní síť.

WAN Wide area network - Rozlehlá datová síť

XSS cross-site scripting.

Přílohy

A Podrobný report TCO

Total Cost of Ownership (TCO) Calculator

Estimate the cost savings you can realize by migrating your workloads to Azure

My saved reports

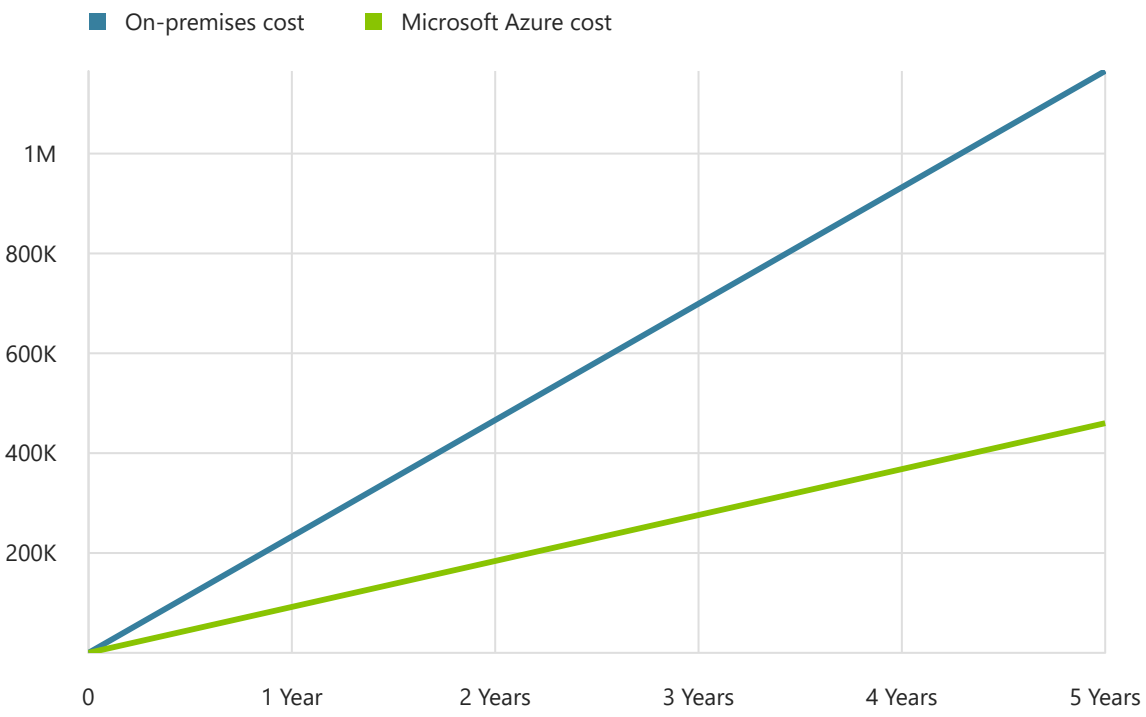
Sign In

Over 5 year(s) with Microsoft Azure, your estimated cost savings could be as much as €705,458

Total on-premises vs. Azure cost over time

Savings from running workloads in Azure accrue over time. The following shows how those savings add up over years.

Chat with Sales



Total on-premises over 5 year(s)

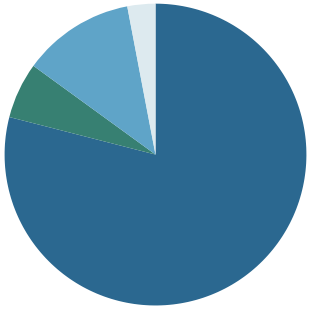
TCO of on-premises environments tends to be driven by compute and data center costs.

Total Azure cost over 5 year(s)

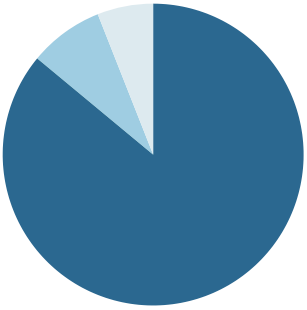
In Azure, certain cost categories decrease or go away completely.

€1,165,493
Total cost

€460,035
Total cost



79% Compute | 6% Data center | 12% Networking | 0% Storage | 3% IT Labor



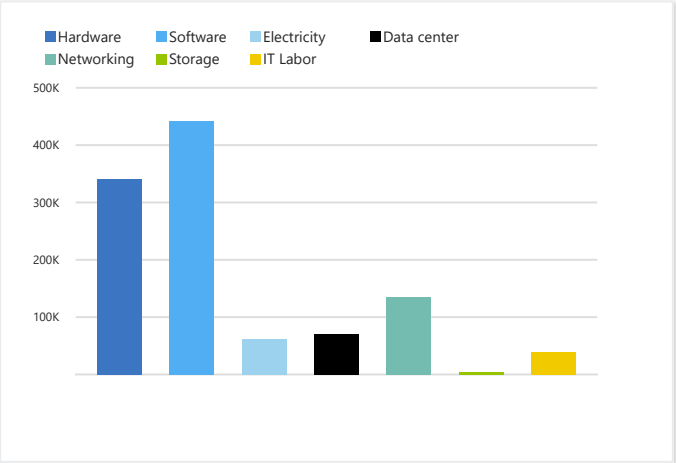
86% Compute | 0% Data center | 0% Networking | 8% Storage | 6% IT Labor

Total on-premises cost breakdown

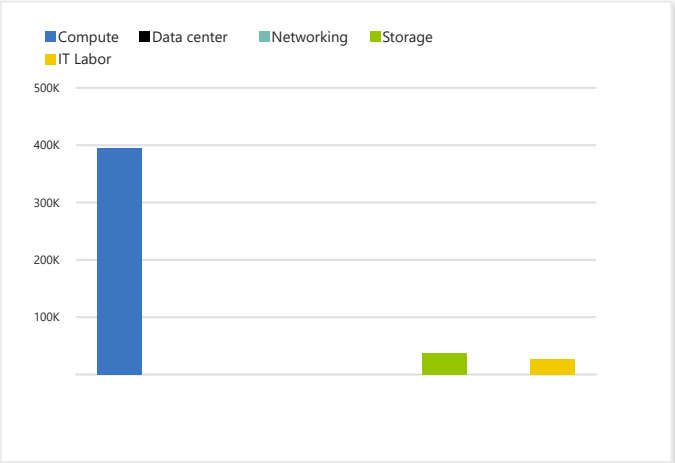
In Azure, several of the cost categories from the on-premises environment are consolidated and decrease with the efficiency that comes with the cloud.

Total Azure cost breakdown

In Azure, several of the cost categories from the on-premises environment are consolidated and decrease with the efficiency that comes with the cloud.



€1,165,493
Cost over 5 year(s)



€460,035
Cost over 5 year(s)

On-premises cost breakdown summary

Category	Cost
Compute	€916,706.65

Azure cost breakdown summary

Category	Cost

Hardware	€341,611.39
Software	€442,712.90
Electricity	€62,333.84
Database	€70,048.51
Data Center	€70,659.50
Networking	€135,304.20
Storage	€3,534.55
IT Labor	€39,288.11
Total	**€1,165,493.33**

Compute	€394,530.56
Data Center	€0.00
Networking	€0.00
Storage	€37,933.23
IT Labor	€27,570.9454
Total	**€460,034.86**

Estimated on-premises cost (5 year(s))

Estimated Azure cost (5 year(s))

Compute cost

Azure compute cost

Hardware cost

Cost per 1 proc 4 core, 7 GB RAM physical server for Windows	€1,754.13
Number of servers required	2
Cost per 1 proc 2 core, 3.5 GB RAM physical server for Windows	€1,514.07
Number of servers required	1
Cost per 2 proc 16 core, 256 GB RAM physical server for Windows	€19,567.81
Number of servers required	5
Cost per 1 proc 4 core, 7 GB RAM physical server for Windows	€1,754.13
Number of servers required	8
Cost per 1 proc 2 core, 3.5 GB RAM physical server for Windows	€1,514.07
Number of servers required	3
Cost per 4 proc 8 core, 448 GB RAM physical server for Windows	€24,684.54
Number of servers required	2
Total cost for physical server(s)	€170,805.70
Cost of maintaining physical server(s) - 20% of cost of physical server(s)	€34,161.14
Total cost of maintaining server(s) over five year(s)	€170,805.70
Total hardware cost over five year(s)	**€341,611.40**

Software cost

Cost of Windows datacenter license per 1 proc, 4 core, 7 GB RAM physical machine	€5,533.91
Number of licenses needed	2

Virtual Machines cost

Number of hours per month	730
B4MS Standard (4 core, 16 GB RAM) Windows (Azure Hybrid Benefit)	SKU# AAA-87170
Number of virtual machines	2
Total virtual machine cost per month	€118.376
	Licensing program: Dev/Test
B2S Standard (2 core, 4 GB RAM) Windows (Azure Hybrid Benefit)	SKU# AAA-87186
Number of virtual machines	1
Total virtual machine cost per month	€14.829
	Licensing program: Dev/Test
M16MS Standard (16 core, 437.5 GB RAM) Windows (Azure Hybrid Benefit)	SKU# AAD-14924
Number of virtual machines	5
Total virtual machine cost per month	€5,732.17
	Licensing program: Dev/Test
B4MS Standard (4 core, 16 GB RAM) Windows (Azure Hybrid Benefit)	SKU# AAA-87170
Number of virtual machines	8
Total virtual machine cost per month	€473.505
	Licensing program: Dev/Test
Windows Server 2008 and 2008 R2 security updates cost	
Extended Security Updates for Windows Server 2008 and 2008 R2	€0.00

Cost of Windows datacenter license per 1 proc, 2 core, 3.5 GB RAM physical machine	€5,533.91
Number of licenses needed	1
Cost of Windows datacenter license per 2 proc, 16 core, 256 GB RAM physical machine	€11,067.82
Number of licenses needed	5
Cost of Windows datacenter license per 1 proc, 4 core, 7 GB RAM physical machine	€5,533.91
Number of licenses needed	8
Cost of Windows datacenter license per 1 proc, 2 core, 3.5 GB RAM physical machine	€5,533.91
Number of licenses needed	3
Cost of Windows datacenter license per 4 proc, 8 core, 448 GB RAM physical machine	€11,067.82
Number of licenses needed	2
Total software license cost	€154,949.52
Total Software Assurance cost	€38,737.38
Extended Security Updates for Windows Server 2008 and 2008 R2 (75% of cost of the license annually for 3 year(s)) Learn more (https://www.microsoft.com/cloud-platform/windows-server-2008)	€249,026.01
Total software cost over five year(s)	**€442,712.90**

Electricity cost

Price of electricity per kWh	€0.15
Power rating of 4 core, 7 GB RAM server	166 Watts
Total electricity cost consumed by 2 server(s) - 4 core, 7 GB RAM server per month	€35.58
Power rating of 2 core, 3.5 GB RAM server	156 Watts
Total electricity cost consumed by 1 server(s) - 2 core, 3.5 GB RAM server per month	€16.71
Power rating of 16 core, 256 GB RAM server	1,002.3 Watts

NOTE: Windows Server 2008 and 2008 R2 virtual machines in Azure receive Extended Security Updates until Jan. 2023 at no additional charge. Learn more (https://www.microsoft.com/cloud-platform/windows-server-2008)

Total Azure Virtual Machines cost	**€380,332.68**

NOTE: For Azure compute costs, 3 year Reserved VM and two 1 year Reserved VM in use.

App Service cost

S2 Standard App Service (2 core, 3.5 GB RAM)	€0.20 /hr
	SKU# T2X-00011
Full time App Service instances	1
Average utilization	80 %
Auto scaling	Yes
Peak Load % per month	40 %
Auto scaled instances	2
Total App Service cost per month	€128.58
	Licensing program: Dev/Test
Total App Service cost over five year(s)	**€7,714.90**

SQL Database cost

Single Standard S2 (Azure Hybrid Benefit)	€0.09250 /hr
	SKU# 4WP-00006
Instance Count	2
Cost Per Month	€54.03
SQL Server 2008 and 2008 R2 security updates cost	
Extended Security Updates for SQL Server 2008 and 2008 R2 Note: SQL Server 2008 and 2008 R2 virtual machines in Azure receive Extended Security Updates until Jan. 2023 at no additional charge.	€0.00

Total electricity cost consumed by 5 server(s) - 16 core, 256 GB RAM server per month	€536.99
Power rating of 4 core, 7 GB RAM server	166 Watts
Total electricity cost consumed by 8 server(s) - 4 core, 7 GB RAM server per month	€142.31
Power rating of 2 core, 3.5 GB RAM server	156 Watts
Total electricity cost consumed by 3 server(s) - 2 core, 3.5 GB RAM server per month	€50.14
Power rating of 8 core, 448 GB RAM server	1,200 Watts
Total electricity cost consumed by 2 server(s) - 8 core, 448 GB RAM server per month	€257.16
Total electricity cost over five year(s)	**€62,333.84**

SQL Database cost

Total CPU cores	16
SQL Server Standard License cost per 2 cores	€3,341.92
Standard cores	16
Total license cost	€26,735.36
Extended Security Updates for SQL Server 2008 and 2008 R2 (75% of cost of the license annually for 3 year(s)) Learn more (https://www.microsoft.com/en-us/sql-server/sql-server-2008)	€12,030.92
Standard Software Assurance cost per 2 cores	€782.06
Standard cores	16
Total Software Assurance cost	€31,282.20
Total SQL Database cost over five year(s)	**€70,048.51**

NOTE: A minimum of four core licenses are required for each physical processor on the server or VM Learn more (https://www.microsoft.com/en-us/sql-server/sql-server-2008)

Total SQL Database cost over five year(s)	**€6,483.00**

Total cost over five year(s)	**€916,706.65**

Total Azure compute cost over five year(s)	**€394,530.56**

Data center cost

Azure data center cost

Total Azure data center cost over five year(s)	€0.00

Compute cost

Number of rack units per rack	42
Rack units required per 4 core, 7 GB RAM server	1
Number of 4 core, 7 GB RAM server	2
Total number of rack units required	€1.83
Rack units required per 2 core, 3.5 GB RAM server	1
Number of 2 core, 3.5 GB RAM server	1
Total number of rack units required	€0.92
Rack units required per 16 core, 256 GB RAM server	4
Number of 16 core, 256 GB RAM server	5
Total number of rack units required	€18.35
Rack units required per 4 core, 7 GB RAM server	1
Number of 4 core, 7 GB RAM server	8
Total number of rack units required	€7.34
Rack units required per 2 core, 3.5 GB RAM server	1
Number of 2 core, 3.5 GB RAM server	3
Total number of rack units required	€2.75
Rack units required per 8 core, 448 GB RAM server	4
Number of 8 core, 448 GB RAM server	2
Total number of rack units required	€7.34
Total number of rack units required for all server(s)	€38.53

Data center construction cost per rack unit amortized over 20 years	€271.77
Data center compute cost	€11,414.23
Total Data center compute cost over five year(s)	**€57,071.10**

Storage cost

Total number of rack units required for all storage	10
Number of rack units for DAS or SAN	10
Rack mounting/installation cost	€2,717.67
Total Data center storage cost over five year(s)	**€13,588.37**

Total Data center cost over five year(s)	**€70,659.50**

Total Azure data center cost over five year(s)	**€0.00**

Networking cost

Total hardware + software cost over five year(s)	€784,324.30
Network hardware and software cost assumed to be 15% of hardware and software cost over five year(s)	€117,648.64
Network maintenance cost assumed to be 15% of network hardware and software cost over five year(s)	€17,647.30
Service provider cost/GB per month	€0.14
Amount of bandwidth needed (GB) per month	1
Total service provider cost per month	€0.14

Azure networking cost

Total outgoing bandwidth needed per month	1 GB
Total outgoing bandwidth cost per month	€0.00

Total networking cost over five year(s)	**€135,304.20**

Total Azure networking cost over five year(s)	**€0.00**

Storage cost

Azure storage cost

Hardware

Local Disk/SAN-HDD	
Cost per GB	€0.19
Storage (RAID 10 configuration) volume in GB	10,240
Total storage procurement cost	**€1,972.80**

Backup

Total backup and archive volume in GB	20,480
	HP LTO-7 BB873A
Backup volume per tape in TB	6
Number of Tape drives required	4
Cost per Tape Drive	€143.86
Backup and Archive cost over five year(s)	**€575.42**

Storage Maintenance

Storage maintenance cost (10% of storage procurement cost) over five year(s)	€986.40
Total storage maintenance cost over five year(s)	**€986.40**

Page Blob storage

Usable storage volume in GB	5,120
Storage cost per GB/month	€0.041
Annual storage cost per usable volume	€2,536.40
Total Page Blob LRS storage maintenance cost over five year(s)	**€12,681.99**

Backup

Total backup and archive volume in GB	20,480
Storage cost per GB	€0.0205
	SKU# AAL-31806
Backup and Archive maintenance cost over five year(s)	**€25,251.25**

year(s)	€3,534.55

Total Azure storage cost over five year(s)	€37,933.23

IT labor cost

Number of IT admin hour(s) needed per year	380
Hourly rate for IT administrator	€20.68
Total IT labor cost over five year(s)	**€39,288.11**

Azure IT labor cost

Number of IT admin hour(s) needed per year	266.67
Hourly rate for IT administrator	€20.68
Total Azure IT labor cost over five year(s)	**€27,570.945**

Total on-premises cost over five year(s)	**€1,165,493.33**
Total Azure cost over five year(s)	**€460,034.86**

A total **savings** of **€705,458.47** with **Microsoft Azure**

Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání diplomové práce

Autor:	**Bc. Leoš Karásek**
Studium:	I2000828
Studijní program:	N1802 Aplikovaná informatika
Studijní obor:	Aplikovaná informatika

Název diplomové práce:	**Návrh a realizace migrace infrastruktury na Microsoft Azure**
Název diplomové práce AJ:	

Cíl, metody, literatura, předpoklady:

Cílem diplomové práce je navrhnout a realizovat migraci podnikové infrastruktury na Microsoft Azure. V teoretické části se autor zaměří na analýzu nedostatků a slabých míst stávající infrastruktury a poskytovaných služeb s důrazem na jejich zabezpečení. Navrhne možnosti řešení s maximálním využitím Microsoft Azure a jeho služeb. V praktické části autor navrhne a v maximální možné míře ověří postupy migrace IT infrastruktury a vhodných služeb na Microsoft Azure.

AGRAWAL, Ashish. *Exam Ref AZ-304 Microsoft Azure Architect Design*. Addison Wesley: Pearson Education (US), 2021. ISBN 9780137268894. PATEL, Harshul. *Exam Ref AZ-104 Microsoft Azure Administrator*. Addison Wesley: Pearson Education (US), 2021. ISBN 9780136805380.

Zadávající pracoviště:	Katedra informačních technologií, Fakulta informatiky a managementu
Vedoucí práce:	doc. Mgr. Josef Horálek, Ph.D.
Datum zadání závěrečné práce:	9.9.2021