Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Cloud computing v sektoru malých a středních podniků

Vojtěch Slavíček

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Vojtěch Slavíček

Informatika

Název práce

Cloud computing v sektoru malých a středních podniků

Název anglicky

Cloud computing in the sector of small and medium-sized companies

---

Cíle práce

Hlavním cílem bakalářské práce bude analýza a porovnání bezpečnostních politik, standardů a konkrétních bezpečnostních opatření u vybraných poskytovatelů cloud computingu pro malé a střední podniky.

Metodika

Pro tvorbu teoretické části bakalářské práce bude využita vědecká a odborná literatura. Zpracovaná literární rešerše bude použita jako základ praktické části, kde pomocí metody komparativní analýzy budou porovnány bezpečnostní politiky, bezpečnostní standardy a konkrétní bezpečnostní opatření u třech největších poskytovatelů cloudových služeb. Následně bude provedeno vyhodnocení a vyhotoveno doporučení pro další možné použití

Doporučený rozsah práce

40 stran

Klíčová slova

cloud computing, cloud, SaaS, PaaS, IaaS, bezpečnost

Doporučené zdroje informací

FAYNBERG,I.,SKULER,D.,LU,H.:Cloud Computing: Business Trends and Technologies,2015,ISBN 9781118501214

KAVIS, M. J.: Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and laaS). 1.edice, p. 247, 2014 , ISBN 978-1118617618

LACKO, Ľuboslav:Osobní cloud pro domácí podnikání a malé firmy,2012,ISBN 978-80-251-3744-4

VELTE, A. T., VELTE, T. J., ELSENPETER, R.: Cloud computing a practical approach. s. 296, 2011, ISBN: 978-80-251-3333- 0

Předběžný termín obhajoby

2023/24 LS – PEF

Vedoucí práce

doc. Ing. Edita Šilerová, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 4. 7. 2023

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 3. 11. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 15. 03. 2024

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Cloud computing v sektoru malých a středních podniků" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.03. 2024 _____

Poděkování

Rád bych touto cestou poděkoval paní doc. Ing. Editě Šilerové, Ph.D. za cenné rady a odborné vedení při zpracování této bakalářské práce.

Cloud computing v sektoru malých a středních podniků

Abstrakt

Předmětem bakalářské práce je cloud computing v sektoru malých a středních podniků. V úvodních stránkách teoretické části se práce zabývá definicí cloud computingu, jeho historií a popisem základních charakteristik. Dále se věnuje modelům nasazení a distribučním modelům cloud computingu včetně jejich výhod a nevýhod a komponentům cloudu. V závěru teoretické části se zaměřuje na cloudovou bezpečnost, bezpečnostní rizika a hrozby, zásady správného zabezpečení cloudu a definici sektoru malých a středních podniků.

V praktické části se práce zabývá představením tří největších poskytovatelů cloudových služeb a jejich porovnáním na základě čtyř kritérií zaměřených na bezpečnost. Na základě těchto porovnání byla vyhotovena vícekriteriální analýza variant a závěr praktické části je věnován shrnutí výsledků a doporučení pro firmy ze sektoru malých a středních podniků.

Klíčová slova: cloud computing, SaaS, PaaS, IaaS, cloud, bezpečnost, Amazon, Microsoft, Google

Cloud computing in the sector of small and medium-sized companies

Abstract

The subject of the bachelor thesis is cloud computing in the SME sector. In the introductory pages of the theoretical part, the thesis deals with the definition of cloud computing, its history and description of its basic characteristics. It then discusses the deployment and distribution models of cloud computing including their advantages and disadvantages and the components of the cloud. The theoretical part concludes with a focus on cloud security, security risks and threats, principles of proper cloud security and a definition of the SME sector.

In the practical part, the thesis introduces the three largest cloud service providers and compares them based on four security-focused criteria. Based on these comparisons, a multiple-criteria decision analysis was performed and the practical part concludes with a summary of the results and recommendations for companies in the SME sector.

Keywords: cloud computing, SaaS, PaaS, IaaS, cloud, security, Amazon, Microsoft, Google

Obsah

1 Úvod **11**

2 Cíl práce a metodika **12**

2.1 Cíl práce 12

2.2 Metodika 12

3 Teoretická východiska **13**

3.1 Cloud computing 13

3.1.1 Historie 13

3.1.2 Základní charakteristiky 14

3.2 Modely nasazení 16

3.2.1 Veřejný cloud (Public cloud) 16

3.2.2 Privátní cloud (Private cloud) 17

3.2.3 Komunitní cloud (Community cloud) 18

3.2.4 Hybridní cloud (Hybrid cloud) 19

3.3 Distribuční modely 19

3.3.1 SaaS (Software as a Service) 20

3.3.2 PaaS (Platform as a Service) 21

3.3.3 IaaS (Infrastructure as a Service) 22

3.4 Komponenty cloudu 23

3.4.1 Klienti 24

3.4.2 Datová centra 24

3.4.3 Distribuované servery 25

3.5 Bezpečnost 25

3.5.1 Základní kategorie cloudového zabezpečení 26

3.5.2 Bezpečnostní rizika a hrozby 28

3.5.3 Zásady správného zabezpečení cloudu 30

3.6 Sektor malých a středních podniků 30

4 Vlastní práce **32**

4.1 Představení poskytovatelů 32

4.1.1 Amazon 32

4.1.2 Microsoft 32

4.1.3 Google 33

4.2 Komparativní analýza 33

4.2.1 Kritérium 1. – Standardy, certifikace a právní předpisy 33

4.2.2 Kritérium 2. - Fyzické zabezpečení datových center 36

4.2.3 Kritérium 3. – Šifrování dat v klidu 41

4.2.4 Kritérium 4. - Reakce na bezpečnostní incidenty 46

4.3 Vícekriteriální analýza variant 49
4.3.1 Stanovení vah kritérií 49
4.3.2 Seřazení jednotlivých variant 50

5 Výsledky 52
5.1 Doporučení 52

6 Závěr 54

7 Seznam použitých zdrojů 55
7.1 Literární zdroje 55
7.2 Internetové zdroje 55

8 Seznam obrázků, tabulek, grafů a zkratek 60
8.1 Seznam obrázků 60
8.2 Seznam tabulek 60
8.3 Seznam grafů 60
8.4 Seznam použitých zkratek 60

1 Úvod

Cloud computing se stal neodmyslitelnou součástí informačních technologií, transformující způsob, jakým firmy a jednotlivci pracují s daty a aplikacemi. Přestože značná část společnosti stále nemá ponětí o jeho existenci, pravděpodobně se s jeho službami setkává každý den, aniž by si to uvědomovala.

Tento výpočetní model, fungující na bázi internetu umožňuje firmám i jednotlivcům vzdálený přístup ke zdrojům a jejich rychlé a flexibilní škálování. Odstraňuje potřebu vlastnictví a údržby fyzické infrastruktury a umožňuje tak podnikům snížit náklady a zvýšit efektivitu. Podniky mohou jednoduše přizpůsobit své IT prostředky měnícím se podmínkám bez nutnosti nákladných investic do serverů či hardwaru.

Existují však i výzvy, zejména v oblasti bezpečnosti dat a ochrany soukromí, kdy výběr důvěryhodného poskytovatele a adekvátní bezpečnostní opatření jsou klíčovým způsobem, jak těmto výzvám čelit.

Tato práce se skládá ze dvou částí. Teoretická část je věnována definici cloud computingu, jeho historii a základním charakteristikám. Dále obsahuje modely cloud computingu a jejich výhody a nevýhody, komponenty cloudu, cloudovou bezpečnost a definici sektoru malých a středních podniků. V praktické části jsou nejprve představeni a poté porovnáni tři největší poskytovatelé cloudových služeb z hlediska kritérií zaměřených na bezpečnost.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem bakalářské práce je analýza a porovnání bezpečnostních politik, standardů a konkrétních bezpečnostních opatření u vybraných poskytovatelů cloud computingu pro malé a střední podniky. Dílčím cílem je poskytnout souhrnný přehled o bezpečnostních aspektech u vybraných poskytovatelů cloud computingu. Dalším dílčím cílem je zpracování literární rešerše na základě studia sekundárních zdrojů a vědecké a odborné literatury.

2.2 Metodika

Pro tvorbu teoretické části bakalářské práce byla využita vědecká a odborná literatura. Zpracovaná literární rešerše byla použita jako základ praktické části, kde pomocí metody komparativní analýzy byly porovnány bezpečnostní politiky, bezpečnostní standardy a konkrétní bezpečnostní opatření u třech největších poskytovatelů cloudových služeb. Na základě této analýzy pak byla vypracována vícekriteriální analýza variant, kde byla pro stanovení vah kritérií použita metoda pořadí a seřazení variant bylo provedeno metodou pořadí s váhami. Následně bylo provedeno vyhodnocení a vyhotoveno doporučení pro další možné použití.

3 Teoretická východiska

3.1 Cloud computing

Definovat cloud computing je poměrně složité. Neexistuje totiž jednoznačná definice, na které by se shodla většina odborníků. Za klasickou lze považovat definici od National Institute of Standards and Technology (Murugesan, Bojanova, 2016). V té jsou zahrnuty klíčové prvky i charakteristiky cloud computingu. Definice od NIST zní takto (Mell, Grance, 2011, s. 2): *„Cloud computing je model, který umožňuje všudypřítomný, praktický a síťový přístup na vyžádání ke sdíleným konfigurovatelným zdrojům (např. sítě, servery, úložiště, aplikace a služby), které lze rychle alokovat a odebrat s minimálním úsilím managementu nebo minimální interakcí s poskytovatelem služby. Tento cloudový model se skládá z pěti základních charakteristik, tří distribučních modelů a 4 modelů nasazení“.*

S podobnou definicí přišla The International Organization for Standardization: *„Cloud computing je paradigma, které umožňuje síťový přístup ke škálovatelnému a elastickému souboru sdílených fyzických nebo virtuálních zdrojů se samoobslužným alokováním a správou na vyžádání“* (ISO/IEC DIS 17789:2014, 2014 cit. podle Murugesan, Bojanova, 2016).

Dle společnosti Gartner Inc. je cloud computing: *„Styl výpočetní techniky, kde škálovatelné a elastické zdroje jsou poskytovány jako služba více zákazníkům prostřednictvím internetu“* (Gartner, c2023).

Po shrnutí těchto definic lze dospět k závěru, že cloud computing umožňuje přístup ke vzdáleným zdrojům, které mohou být fyzické či virtuální. Tyto zdroje jsou přístupné pomocí internetu odkudkoliv a lze je relativně snadno přidělovat a odebírat dle potřeby. Uživatelé zdroje nevlastní, ale pouze si je propůjčují. Poskytovanými zdroji mohou být např. cloudová úložiště, servery, síťové infrastruktury, kancelářské aplikace, operační systémy apod.

3.1.1 Historie

Bairagi a Bang (2015) uvádí, že i když se na první pohled může zdát, že cloud computing je relativně nový model, existuje ve světě výpočetní techniky již poměrně dlouhou dobu. Jeho kořeny sahají do roku 1961, kdy John McCarthy jako první vyslovil myšlenku, že výpočetní technologie by jednoho dne mohly být organizovány obdobně jako veřejné služby. O 5 let později byly poprvé popsány charakteristiky cloud computingu v knize The Challenge of the Computer Utility, jejímž autorem je Douglas Parkhill.

Foote (2021) tvrdí, že byl v roce 1969 spuštěn projekt ARPANET (Advanced Research Projects Agency Network), na jehož vývoji se podílel i J. C. R. Licklider. Ten již ve své době propagoval vizi, ve které budou všichni lidé na světě propojeni prostřednictvím počítačů a budou mít přístup k informacím odkudkoli. Vize, kterou nazval Intergalactic Computer Network může částečně připomínat současný internet.

S evolucí internetu se vyvíjel také koncept virtualizace, přičemž rostoucí popularita virtuálních počítačů v 90. letech 20. století umožnila vývoj moderní infrastruktury cloud computingu (Foote, 2021).

Samotný pojem "cloud computing" se pravděpodobně poprvé objevil na přednášce Ramnatha Chellappa, kterou přednesl v roce 1997 (Threat Intel, 2018). Definoval ho jako *„Počítačové paradigma, kde hranice výpočetní techniky budou určovány spíše ekonomickými důvody, než technickými limity"* (Chellappa, 1997 cit. podle Threat Intel, 2018). Nicméně existuje záznam, že termín "cloud computing" se objevil již v roce 1996 v obchodním plánu společnosti Compaq. Pravý původ tohoto výrazu je tedy diskutabilní (Threat Intel, 2018).

Podle Foote (2021) další zlom nastal v roce 1999, kdy společnost Salesforce začala poskytovat programy prostřednictvím internetu koncovým uživatelům. Zjednodušeně řečeno kdokoli s přístupem k internetu mohl programy používat a stahovat je. Firmy si mohly zakoupit programy vysoce efektivním způsobem z hlediska nákladů, ve formě služby na vyžádání.

V historii cloud computingu také hraje klíčovou roli společnost Amazon (Aktuálně.cz, 2011). Dle (Aktuálně.cz, 2011; Foote, 2021) dříve bylo běžné, že firmy využívaly pouze 10% kapacity výpočetní techniky a Amazon se tento problém rozhodl vyřešit nabídnutím nevyužité kapacity zákazníkům. V roce 2006 Amazon spustil Amazon Web Services, vlastní cloudovou službu, která poskytuje online služby dalším webovým stránkám či klientům. Ve stejném roce se připojil i Google, který spustil svoji cloudovou službu s názvem Google Docs services (Foote, 2021). Později také své cloudové služby spustili v dnešní době již velcí poskytovatelé cloudových služeb firmy Microsoft, IBM, Alibaba atd.

3.1.2 Základní charakteristiky

Dle NIST by měl cloud computing splňovat 5 základních charakteristik (Mell, Grance, 2011):

- Samosprávu na vyžádání (On demand self-service);

- Přístup z rozsáhlé sítě (Broad network access);
- Sdílené zdroje (Resource pooling);
- Rychlou elasticitu (Rapid elasticity);
- Měřené služby (Measured service).

Samospráva na vyžádání (On-demand self-service)

Obecně lze říci, že cloud computing má velice rozsáhlé kapacity zdrojů výpočetní techniky a díky tomu je možné bez problému poskytovat uživatelům přístup ke zdrojům na vyžádání. Vzhledem k rozsáhlým kapacitám často vzniká iluze, že zdroje jsou neomezené a lze je zakoupit v libovolném množství. Nic ale není neomezené, a to platí i u cloud computingu. Nicméně uživatelé si mohou zakoupit dostatečné množství zdrojů, které uspokojí jejich potřeby, kdykoli, bez interakce s poskytovatelem cloudové služby (Yang, Huang, 2013).

Přístup z rozsáhlé sítě (Broad network access)

Tato charakteristika ve zkratce znamená, že ke zdrojům cloud computingu je možné přistupovat pomocí internetu ze standardních zařízení, jako např. mobilních telefonů, notebooků, stolních počítačů apod. Všechna zařízení navzdory jejich různorodosti mohou pracovat se stejnou verzí dat po připojení k internetu, díky automatické synchronizaci dat v cloudu (Yang, Huang, 2013).

Sdílené zdroje (Resource pooling)

Dle Yanga a Huanga (2013) jsou výpočetní zdroje poskytovatele cloudových služeb sdíleny mezi uživateli v rámci modelu s více nájemci. Velkou roli zde hraje poptávka uživatelů, na jejímž základě jsou virtuální zdroje dynamicky přiřazovány a odebírány. Z pohledu uživatelů tento model sdílených zdrojů založený na virtualizaci znamená nižší náklady na koupi, provoz a údržbu výpočetních zdrojů. Dalším plusem pro uživatele je, že se nemusí starat o infrastrukturu, jelikož veškeré povinnosti spojené s provozem a údržbou jsou outsourcovány na poskytovatele. Ale i pro poskytovatele jsou virtualizační technologie velkým přínosem. Díky nim totiž mohou zakomponovat nejnovější fyzické zdroje mezi zdroje sdílené a snížit tak náklady na údržbu a mimo jiné také upgradovat cloudovou platformu. Takovým typickým příkladem sdílených zdrojů je úložiště, zpracování dat a paměť (Mell, Grance, 2011).

Rychlá elasticita (Rapid elasticity)

Yang a Huang (2013) poukazují na to, že aplikace poskytované skrze cloudové služby lze nastavit tak, že v případě zvýšeného pracovního zatížení budou elasticky získávat více prostředků a nedojde tak ke snížení výkonu. Totéž platí samozřejmě i zpětně, tedy pokud dojde k poklesu pracovního zatížení prostředky mohou být velmi rychle uvolněny, konkrétně v řádu několika sekund až minut.

Měřené služby (Measured service)

Poskytovatelé cloudových služeb hojně využívají flexibilní cenové modely. Velmi často nabízí uživatelům možnost hodinové platby, tedy uživatel zaplatí za cloudové služby podle počtu hodin, po které služby využíval, bez jakéhokoli dlouhodobého závazku vůči poskytovateli (Yang, Huang, 2013). Za účelem zvýšení transparentnosti, jak pro uživatele, tak pro poskytovatele může být využívání cloudových služeb monitorováno, kontrolováno a hlášeno (Mell, Grance, 2011).

3.2 Modely nasazení

Kumar (2023) tvrdí, že výraz model nasazení lze interpretovat jako virtuální výpočetní prostředí, které se určuje na základě toho, kdo všechno bude mít přístup k infrastruktuře a jak velké množství dat budou uživatelé ukládat. Obecně se rozlišují 4 modely nasazení (Kumar, 2023):

- Veřejný cloud (Public cloud);
- Privátní cloud (Private cloud);
- Komunitní cloud (Community cloud);
- Hybridní cloud (Hybrid cloud).

3.2.1 Veřejný cloud (Public cloud)

Podle Kumara (2023) je typickým znakem veřejného cloudu jeho dostupnost pro širokou veřejnost. Je k dispozici v podstatě pro kohokoli s přístupem k internetu. Také vzhledem k tomu je veškerá správa a provoz veřejného cloudu zajištěna poskytovatelem cloudu, který je rovněž vlastníkem poskytovaných cloudových prostředků (Microsoft, c2023). Z hlediska financí uživatelé platí pouze za jimi využívané služby. Možná také proto je veřejný cloud s největší pravděpodobností nejvíce populární a nejvyspělejší typ cloudu

(Yang, Huang, 2013). Skrze veřejný cloud jsou nejčastěji poskytovány online kancelářské aplikace, testovací a vývojová prostředí, email a úložiště (Microsoft, c2023).

Výhody

Dle Kumara (2023) je velkou výhodou veřejného cloudu bezpochyby **správa infrastruktury**. Jak je výše uvedeno o veškerou správu a provoz cloudu se stará poskytovatel, což je výhodné především pro uživatele. Další výhodou je **vysoká škálovatelnost**, která umožňuje uživatelům snižovat a navyšovat prostředky dle jejich aktuální potřeby. Výhodou jsou také relativně **nízké náklady**, jelikož uživatelé platí pouze za jimi využívané služby a nemusí si pořizovat své vlastní prostředky (Microsoft, c2023).

Nevýhody

Bezpečnost dat a soukromí jsou velmi důležitá kritéria, dalo by se říct pro všechny uživatele cloudových služeb, proto fakt, že v případě veřejného cloudu více uživatelů využívá stejné prostředky může u některých vyvolat obavy týkající se bezpečnosti a soukromí. Veřejný cloud také není úplně nejlepší volba pro uživatele, kteří běžně pracují na složitých úkolech, kvůli jistým **omezením služeb a licencí**. Nabízené služby jsou totiž obecné a nemusí být pro náročnější uživatele dostačující (Kumar, 2023).

3.2.2 Privátní cloud (Private cloud)

Na rozdíl od veřejného cloudu je privátní cloud vyhrazen pouze pro jednu firmu či organizaci, tzn. veškeré prostředky využívá pouze tato firma nebo organizace a nesdílí je s nikým dalším (Yang, Huang, 2013; Kumar, 2023). Co se týče umístění privátního cloudu, Microsoft (c2023) tvrdí, že může být umístěn fyzicky v datovém centru organizace, nebo existuje též možnost hostování poskytovatelem cloudových služeb. Dalším důležitým atributem privátního cloudu je, že služby a infrastruktura jsou udržovány v privátní síti a každá organizace má zajištěný hardware a software čistě pro sebe. Organizace také mají možnost zachovat si absolutní kontrolu nad svými prostředky (Yang, Huang, 2013).

Privátní cloud je hojně využíván ve vládních agenturách, finančních institucích a ve středně velkých až velkých organizacích, pro které je nezbytná zvýšená kontrola nad svým prostředím (Microsoft, c2023).

Výhody

(Kumar, 2023; Microsoft, c2023) poukazují na to, že vzhledem k nesdíleným prostředkům mohou firmy snadněji docílit **větší kontroly** nad prostředky a větší úrovně ochrany osobních údajů. Silnou stránkou privátního cloudu je i **vysoká škálovatelnost a flexibilní možnosti nasazení**. Cloudové prostředí lze totiž modifikovat tak, aby bylo v souladu s konkrétními obchodními potřebami.

Nevýhody

Velkým mínusem jsou bezpochyby **vysoké náklady**, způsobené interní údržbou infrastruktury, která vyžaduje proškolení zaměstnanců a je mimo jiné rovněž zodpovědná za velké výdaje na hardware a software. Z tohoto důvodu není privátní cloud úplně nejšťastnějším výběrem pro malé společnosti. Mínusem je také, že i přes dříve zmiňovanou vysokou škálovatelnost je její výše **závislá** na zvoleném hardwaru (Kumar, 2023).

3.2.3 Komunitní cloud (Community cloud)

Komunitní cloud má z dříve představených modelů nejblíže k privátnímu cloudu (Kumar, 2023). Na rozdíl od privátního cloudu je však navržen tak, aby sloužil více společnostem se stejnými zájmy (Yang, Huang, 2013). Nevlastní ho tedy jedna firma, ale je sdílen mezi více společnostmi (Kumar, 2023). Ohledně provozu a správy cloudu zde existuje více možností, buď má na starost provoz a správu poskytovatel třetí strany, nebo je vše zajištěno interně (Yang, Huang, 2013).

Výhody

Sdílení cloudového prostoru mezi více firmami pomáhá **snižovat náklady**, protože se na financování cloudu podílí několik firem, mezi které jsou náklady rozděleny. Jako další výhoda se nabízí **snadná spolupráce a sdílení dat** mezi firmami. Dalo by se i říci, že z tohoto důvodu byl komunitní cloud v první řadě vůbec navržen (Kumar, 2023).

Nevýhody

Nevýhodou komunitního cloudu jsou časté problémy s **nižší kapacitou šířky pásma s omezeným úložištěm** a jako nevýhodu lze též označit **vyšší náklady** oproti veřejnému cloudu (Kumar, 2023).

3.2.4 Hybridní cloud (Hybrid cloud)

Jak už název vypovídá, hybridní cloud kombinuje 2 nebo více z již dříve zmíněných modelů nasazení, za účelem dosažení specifických potřeb, např. obchodních požadavků na dodržování právních předpisů, maximálního využití investic do místních technologií, řešení problémů s nízkou latencí atd. (Microsoft, c2023; Yang, Huang, 2013). Spousta společností využívá hybridní cloud v kombinaci veřejného cloudu, ve kterém jsou ukládána méně citlivá data a privátního cloudu, kde jsou uchovávána citlivá data (Kumar, 2023).

Výhody

Silnou stránkou hybridního cloudu je dle Microsoftu (c2023) jeho **flexibilita**. Společnosti mohou pro zpracování některých úkolů využít prostředky ve veřejném cloudu, zatímco vysoce citlivá data mohou uchovávat v privátním cloudu. S tím se pojí i **nákladová efektivita**, protože v případě škálování na veřejný cloud je účtován další výpočetní výkon pouze, pokud je aktuální výpočetní výkon nedostačující.

Nevýhody

Jelikož je hybridní cloud složen ze 2 a více modelů nasazení, **zřízení hybridního cloudu je poněkud komplikovanější**, protože je nutné vše správně nastavit a z integrovat (Kumar, 2023). Je ale možné si přechod na hybridní cloud usnadnit, a to postupným migrováním a fázovým přesunem úloh v průběhu času (Microsoft, c2023).

3.3 Distribuční modely

Distribuční modely lze rozdělit do 3 primárních kategorií (Murugesan, Bojanova, 2016):

- SaaS (Software as a Service);
- PaaS (Platform as a Service);
- IaaS (Infrastructure as a Service).

Toto dělení je určeno na základě rámce služeb, který je v daném distribučním modelu nabízen. Pro zjednodušení, SaaS nabízí software, PaaS platformu a IaaS infrastrukturu (Murugesan, Bojanova, 2016).

Kromě těchto 3 základních modelů se dnes lze setkat s celou řadou dalších modelů, např. DSaaS (Data Storage as a Service), AaaS (Analytics as a Service), DaaS (Desktop as

a Service), SecaaS (Security as a service), IAMaaS (Identity and Access Management as Service), MaaS (Monitoring as a Service) (Murugesan, Bojanova, 2016).

3.3.1 SaaS (Software as a Service)

Definice SaaS od NIST zní takto (Mell, Grance, 2011, s. 2): *„Schopnost poskytovaná spotřebiteli je používat aplikace poskytovatele běžící na cloudové infrastruktuře. Aplikace jsou přístupné z různých klientských zařízeních buď prostřednictvím rozhraní tenkého klienta, jako je webový prohlížeč (např. webový email), nebo programového rozhraní. Spotřebitel nespravuje ani neřídí základní cloudovou infrastrukturu, včetně sítě, serverů, operačních systémů, úložiště, nebo dokonce individuálních aplikačních schopností, s možnou výjimkou limitovaných nastavení konfigurace aplikací specifických pro uživatele“*.

Distribuční model SaaS lze v podstatě charakterizovat jako model, kde poskytovatel cloudových služeb hostuje aplikaci a poskytuje ji jako službu uživatelům prostřednictvím internetu. To znamená, že uživatelé nemusí aplikaci instalovat na svůj počítač, což je z dlouhodobého hlediska užitečné, poněvadž tak odpadá nutnost upgradovat aplikaci na nejnovější verzi, protože se o vše postará poskytovatel. Na místě nejsou ani obavy z hardwarového hlediska, novější verze aplikace by měly běžet kvalitně, ať už na novějším či starším hardwaru. Co se týče nákladů, tak jejich výše je určena na základě používání daných služeb. Ze začátku, při pořízení tedy není nutné vynaložit velké množství kapitálu, ale za službu je třeba platit dlouhodobě. Jako příklad SaaS lze uvést Webmail a Google Apps (Murugesan, Bojanova, 2016).

Výhody

Vzhledem k tomu, že aplikace jsou poskytovány přes internet, se jako výhoda nabízí **dostupnost.** Aplikace jsou dostupné 24 hodin, 7 dní v týdnu a prostřednictvím webového prohlížeče k nim lze přistupovat z libovolného zařízení, např. z telefonu, notebooku, stolního počítače atd. Kromě dostupnosti je SaaS také **nákladově efektivní**. Jak je výše zmíněno, zpočátku není nutné platit vysoké částky za hardware ani software, náklady jsou totiž převážně dlouhodobějšího charakteru ve formě průběžných plateb. Další výhodou SaaS je **škálovatelnost**. Aplikace je možné snadno škálovat v závislosti na měnících se potřebách společnosti (CompTIA – a).

Nevýhody

Bezpečnostní rizika jsou jednoznačně jednou z nevýhod modelu SaaS. Aplikace jsou samozřejmě zabezpečené samotným poskytovatelem, ale i přesto je dobré nakládat s citlivými daty opatrně. Jako nevýhodu lze označit také **ztrátu kontroly**. Veškeré řízení totiž spadá pod poskytovatele služby a uživatelé jsou tak odkázáni na jeho schopnosti. Někdo může považovat jako nevýhodu i **omezené přizpůsobení**. Důvodem je, že převážná část aplikací poskytuje uživatelům pouze omezené přizpůsobení od poskytovatele (CompTIA – a).

3.3.2 PaaS (Platform as a Service)

Tento distribuční model NIST definoval jako *„Schopnost poskytovaná spotřebiteli je nasazení do cloudové infrastruktury, která zahrnuje spotřebitelem vytvořené nebo získané aplikace, jež byly vytvořené pomocí programovacích jazyků, knihoven, služeb a nástrojů podporovaných poskytovatelem. Spotřebitel nespravuje ani neřídí základní cloudovou infrastrukturu včetně sítě, serverů, operačních systémů, nebo úložiště, ale má kontrolu nad nasazenými aplikacemi a případně i nad konfiguračním nastavení hostitelského prostředí aplikace“* (Mell, Grance, 2011, s. 2-3).

Zatímco v SaaS modelu poskytovatel hostuje aplikace, pro model PaaS je charakteristické, že poskytovatel hostuje platformu a nástroje pro vývoj aplikací a middlewarové systémy, které pak nabízí vývojářům aplikací. Vývojáři tak nemusí přímo interagovat se základní infrastrukturou a mohou se zaměřit jen na kódování a nasazení. Ke většině nástrojů a vybavení, které jsou potřebné pro vývoj a nasazení aplikací a služeb mohou vývojáři přistupovat skrze platformu. Typickými příklady modelu PaaS jsou Google App Engine, Microsoft Azure a Amazon's Web services (Murugesan, Bojanova, 2016).

Výhody

Stejně jako u SaaS je u PaaS velkou výhodou kromě **škálovatelnosti**, která umožňuje dynamicky navyšovat a snižovat prostředky i **nákladová efektivita**. PaaS se též vyznačuje **flexibilitou**. Pracovníci mohou na aplikacích po přihlášení pracovat odkudkoli a kdykoli díky internetu. Kromě předchozích výhod PaaS také pomáhá k rychlejšímu vytvoření a uvedení aplikací na trh (CompTIA – b).

Nevýhody

U PaaS existuje riziko, že uživatelé **nebudou mít možnost změnit** programovací jazyk, programové rozhraní nebo program, který už nepotřebují. Dalším problémem je **kompatibilita**. PaaS nemusí být kompatibilní se všemi stávajícími vývojovými platformami a případné spojení s jinou platformou by mohlo vést ke komplikacím. Je proto velmi důležité si předem ověřit vzájemnou kompatibilitu. Mínusem PaaS je také relativně **velká závislost na poskytovateli** (CompTIA – b).

3.3.3 IaaS (Infrastructure as a Service)

Dle NIST je IaaS *„Schopnost poskytovaná spotřebiteli je zajištění zpracování, úložiště, sítí a dalších základních výpočetních zdrojů, kde je spotřebitel schopen nasadit a provozovat libovolný software, který může zahrnovat operační systémy a aplikace. Spotřebitel nespravuje ani neřídí základní cloudovou infrastrukturu, ale má kontrolu nad operačními systémy, úložištěm a nasazenými aplikacemi; případně omezenou kontrolu nad vybranými síťovými komponenty (např. firewallů hostitele)“* (Mell, Grance, 2011, s. 3).

Jak už název vypovídá, v modelu IaaS je dodávána nezpracovaná infrastruktura jako služba. Pod nezpracovanou počítačovou infrastrukturou si lze představit servery, procesor, úložiště, síťové vybavení a příslušenství datových center. Všechny zmíněné zdroje jsou poskytovatelem plně outsourcovány jako služba uživateli, tzn. uživatelé si zdroje nekupují, ale pouze pronajímají, a to na určitý čas, dle jejich potřeb. Konečná částka za pronajaté zdroje samozřejmě závisí na množství spotřebovaných zdrojů. Příkladem IaaS je třeba Amazon Elastic Compute Cloud (E2C), GoGrid a FlexiScale (Murugesan, Bojanova, 2016).

Výhody

Z modelu IaaS můžou značně profitovat společnosti, které nečekaně zažívají rychlý růst, ale nemají dostatečné množství finančních prostředků na investice do vlastního hardwaru. Uživatelé totiž **platí pouze za výpočetní zdroje, které používají** a poplatky jsou obvykle účtovány jako měsíční provozní výdaj, tudíž **není nutné vynaložit najednou velké množství kapitálu**. Dále model IaaS disponuje **dynamickým škálováním** a **samoobslužným zřizováním** za pomoci internetu (CompTIA – c).

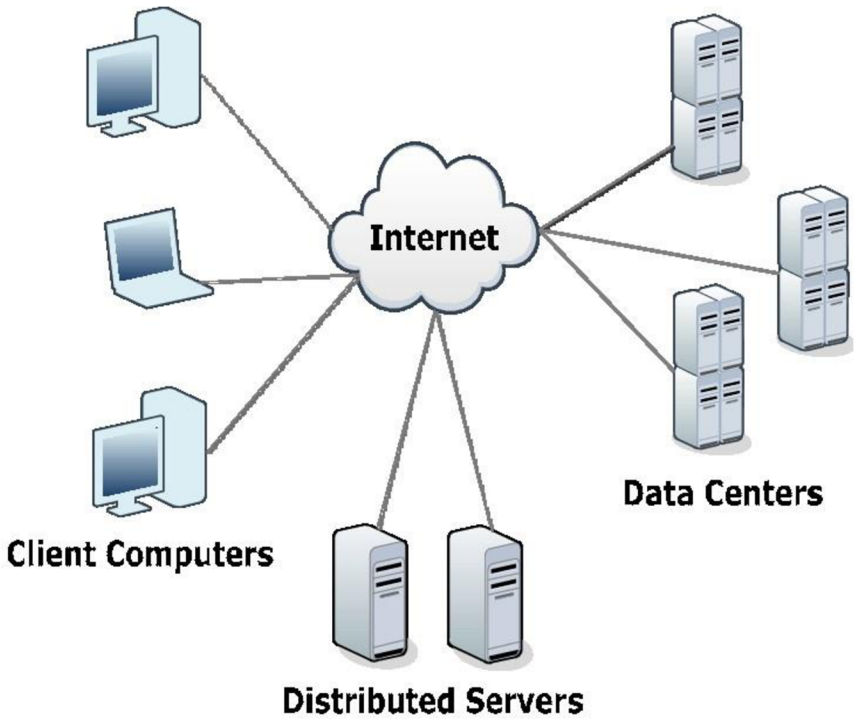
Nevýhody

I přes všechna pozitiva ohledně nákladů, se může stát, že uživatele překvapí **nečekaně vysoké náklady**, způsobené především větším využití zdrojů ve vysokém pracovním nasazení, než se předpokládalo. Dále je také možné, že v rámci nasazení modelu IaaS mohou být vyžadovány **změny v pracovních postupech a procesech**. U některých poskytovatelů se lze navíc setkat s **nedostatečnou podporou**, kdy je někdy obtížné sehnat živou podporu. Kromě těchto nevýhod mohou nastat problémy i v případě **migrace k jinému poskytovateli** IaaS a **složitější integrace** (CompTIA – c).

3.4 Komponenty cloudu

Obecně je cloud computing sestaven ze tří základních komponentů: klientů, datových center a distribuovaných serverů. Všechny tyto komponenty jsou nezbytné pro správné fungování cloudových aplikací, jelikož každý komponent plní svůj účel a svou specifickou roli. Na obrázku 1 je zobrazeno řešení cloud computingu zahrnující zmíněné komponenty (Velte, Velte, Elsenpeter, 2010).

Obrázek 1 Řešení cloud computingu 3 základními komponenty



Zdroj: Shameem, Shaji (2013)

3.4.1 Klienti

Klientem se rozumí zařízení, které vyloženě patří koncovým uživatelům, kteří s ním interagují a jeho prostřednictvím spravují informace v cloudu. Nejčastějšími klientskými zařízeními jsou stolní počítače, notebooky, mobilní telefony a tablety. Obecně lze klienty rozdělit do 3 základních kategorií: mobilní, tenké a tlusté klienty (Velte, Velte, Elsenpeter, 2010).

Mobilní klient

Mobilním klientem mohou být klasické mobilní telefony jako třeba Samsung, iPhone a Huawei, ale i PDA zařízení (Velte, Velte, Elsenpeter, 2010). Pro přístup ke cloudu je však nutné, aby telefon umožňoval připojení k internetu.

Tenký klient

Tenkého klienta je možné charakterizovat jako počítač bez vnitřně zabudovaného pevného disku (Velte, Velte, Elsenpeter, 2010). Všeobecně lze říci, že je to virtuální počítač, který pro svůj chod využívá prostředky uložené na centrálním serveru namísto svých vlastních. Často se tedy jedná o levné zařízení (Gillis, 2021).

Tlustý klient

Tlustý klient je na rozdíl od tenkého klienta počítač s vlastním pevným diskem, který se do cloudu připojuje prostřednictvím internetového prohlížeče (Velte, Velte, Elsenpeter, 2010). Obsahuje většinu základních komponentů, proto není nutné nepřetržité spojení se serverem. Jedná se o plnohodnotný počítač, z hlediska nákladů tedy vyjde oproti tenkému klientovi dráž (Gillis, 2020).

3.4.2 Datová centra

Datové centrum je zjednodušeně soubor serverů, který slouží pro umístění cloudových aplikací. Může existovat v několika podobách, třeba jako velká místnost, která se nachází přímo ve firemní budově. Dost často je datové centrum umístěno také mimo firemní budovu, klidně i v jiné zemi. Takové datové centrum je pak přístupné prostřednictvím internetu (Velte, Velte, Elsenpeter, 2010).

Díky rostoucímu trendu virtualizace serverů je možné po nainstalování softwaru použití více instancí virtuálních serverů. Na jednom fyzickém serveru tak dokáže běžet několik virtuálních serverů (Velte, Velte, Elsenpeter, 2010).

3.4.3 Distribuované servery

Umístění serverů je relativně flexibilní, nemusí být totiž na stejném místě což je velmi často využíváno poskytovateli, kteří umisťují servery na geograficky odlišná místa. Z pohledu uživatelů, se servery však chovají, jako kdyby byly přímo vedle sebe. Pro poskytovatele způsob rozmístění serverů na odlišných místech je výhodný zejména kvůli stabilitě, např. pokud by na některém místě se servery došlo k nějakému selhání, výpadku či poruše, služby by stále byly přístupné z jiného místa. Dále je to pro poskytovatele výhodné v případě navyšování prostředků cloudu (Velte, Velte, Elsenpeter, 2010).

3.5 Bezpečnost

Dle Kaspersky (c2023) cloudová bezpečnost spadá pod kybernetickou bezpečnost a jejím hlavním cílem je zabezpečení systémů cloud computingu. S tím se pojí i snaha o zachování soukromí a bezpečnosti dat v online infrastruktuře, aplikacích a platformách. V podstatě je to ucelený soubor technologií, protokolů a osvědčených postupů, který zajišťuje bezpečnost cloud computingu, od cloudového prostředí, přes aplikace běžící v cloudu, až po uchovávaná data v cloudu. Za zabezpečení cloudu jsou do určité míry zodpovědní poskytovatel cloudu i uživatel a pochopení této skutečnosti je nezbytné pro správné zabezpečení cloudu. Bez ohledu na rozdílné povinnosti zabezpečení ze strany poskytovatele a uživatele, by měly být zabezpečeny vždy tyto položky (Kaspersky, c2023):

- Fyzické sítě;
- Datová úložiště;
- Datové servery;
- Rámce počítačové virtualizace;
- Operační systémy;
- Middleware;
- Běhová prostředí;
- Data;
- Aplikace;
- Hardware koncových uživatelů.

Před implementováním jakéhokoli bezpečnostního opatření je nejprve potřeba určit, co dané opatření bude řešit. Není možné si poradit s každou situací, ale každé bezpečnostní opatření by mělo počítat minimálně s jedním z těchto případů (Kaspersky, c2023):

- Povolení obnovy dat v případě jejich ztráty;
- Ochrana úložiště a sítě před škodlivými krádežemi dat;
- Zamezení lidských chyb nebo nedbalostí, jenž způsobují úniky dat;
- Snížení dopadu jakéhokoli ohrožení dat nebo systému.

3.5.1 Základní kategorie cloudového zabezpečení

Samotné zabezpečení cloudu se skládá z 5 hlavních kategorií: bezpečnosti dat, správy identit a přístupů (IAM), zásad správného řízení, plánování uchovávání dat a kontinuity podnikání a dodržování právních předpisů (Kaspersky, c2023).

Bezpečnost dat

Tato kategorie zastřešuje technickou stránku prevence hrozeb. Existuje řada nástrojů a technologií, pomocí kterých poskytovatelé i klienti mohou přidávat překážky mezi přístup k citlivým údajům a jejich viditelnost. Příkladem může být šifrování, které je považováno za jeden z nejvíce účinných nástrojů. To funguje ve zkratce tak, že se data zašifrují do nečitelné podoby a následně jsou čitelná pouze pro toho, kdo má šifrovací klíč. V případě ztráty či krádeže dat je tak zajištěno, že data budou v šifrované podobě nečitelná a bezvýznamná. Často jsou také používány nástroje, které chrání data již při přenosu, jako např. virtuální privátní sítě VPN (Kaspersky, c2023).

Správa identit a přístupů (IAM)

Součástí správy identit a přístupů je kromě správy autentizace a autorizace uživatelských účtů také nějaký souhrn oprávnění přístupnosti, který je přidělen uživatelským účtům. Řízení přístupu je důležitým prvkem zabezpečení, protože umožňuje omezit a znesnadnit přístup legitimním uživatelům či uživatelům s nekalými úmysly k citlivým datům a systémům a zabránit tak jejich kompromitaci. Mezi další známé metody, které lze zařadit pod správu identit a přístupů patří třeba správa hesel a vícefaktorová autentizace (Kaspersky, c2023).

Zásady správného řízení

Zásady správného řízení se týkají především zásad pro prevenci, detekci a zmírňování dopadů hrozeb. Informace o hrozbách jsou podstatné zejména pro podniky, který díky nim mohou lépe sledovat a následně stanovit priority hrozeb, což je klíčové především pro správné zabezpečení důležitých systémů. Ve firemních prostředích jsou také často adaptovány zásady bezpečného chování uživatelů a někdy jsou i pořádána školení pro zaměstnance ohledně bezpečnosti. Ze zásad správného řízení mohou nicméně těžit všichni uživatelé, nejenom firmy (Kaspersky, c2023).

Plánování uchovávání dat a kontinuity podnikání

Pro případ, že by došlo k nějaké technické havárii a následné ztrátě dat je důležité přijmout opatření týkající se obnovy dat. Zálohování je takovým typickým příkladem, ale existuje řada dalších metod redundance dat. Co se týká kontinuity podnikání, zde mohou být užitečné technické systémy pro zajištění nepřetržitého provozu, rámce pro testování platnosti záloh a podrobné instrukce ohledně obnovy pro zaměstnance (Kaspersky, c2023).

Dodržování právních předpisů

Citlivé údaje uživatelů jsou velmi cenná data, která se dají jednoduše zneužít za účelem zisku. To je jedním z důvodů proč legislativní orgány stanovily právní předpisy týkající se ochrany soukromí především uživatelů. Podniky musí tyto právní předpisy dodržovat, jinak jim hrozí právní postihy. Jako příklady takových právních předpisů lze uvést obecné nařízení o ochraně osobních údajů GDPR v Evropské unii a zákon o odpovědnosti za přenos údajů o zdravotním pojištění HIPAA ve Spojených státech amerických. Pro zajištění souladu se zmíněnými právními předpisy samozřejmě existuje více přístupů, jednou z mnoha používaných metod, která pomáhá zajistit soulad s GDPR je maskování dat, které odděluje identifikovatelné prvky od uživatelských dat. V případě HIPAA si musí některé organizace, např. zdravotnická zařízení dokonce zajistit, aby jejich poskytovatel rovněž omezoval přístup k datům v souladu s HIPAA (Kaspersky, c2023).

Ve spojených státech existuje také zákon Cloud Act, který stanovuje poskytovatelům cloudových služeb právní omezení, jenž musí respektovat. Je zde ale otázka, jak moc velký dopad mají tyto právní omezení na soukromí uživatelů. Dle tohoto zákona si totiž orgány činné v trestním řízení na federální úrovni mohou vyžádat data uložená na serverech

poskytovatelů, zejména za účelem vyšetřování. Kromě obcházení některých práv na soukromí může tedy dojít i k zneužití pravomoci (Kaspersky, c2023).

3.5.2 Bezpečnostní rizika a hrozby

Externí hrozby, interní hrozby, lidské chyby, rizika cloudové infrastruktury, to vše lze označit jako běžná rizika a hrozby, kterým mohou být poskytovatelé a uživatelé cloudových služeb vystaveni (Kaspersky, c2023). Pečlivá identifikace rizik a hrozeb je proto klíčová pro správné zabezpečení cloudových systémů.

Úniky dat

Pod únikem dat si lze představit neoprávněný přístup k informacím. Úniky dat mají ve většině případů na svědomí kyberzločinci, kteří útočí převážně na poskytovatele cloudových služeb, tedy konkrétně na obrovské množství dat uložené na jejich serverech. Nejvíce ohrožená data jsou např. lékařské dokumenty, finanční záznamy a informace o zákaznících (Stouffer, 2023).

Hijacking

Hijacking je typ kybernetického útoku, při kterém útočník získá přístup a následnou kontrolu např. nad systémem, programem, ale třeba i nad cloudovým účtem. K hijackingu často dochází prostřednictvím phishingu a botnetů, a pokud je útok úspěšný, útočníkům nic nebrání v krádeži přihlašovacích údajů či dokonce vysoce citlivých dat a souborů (Stouffer, 2023).

Infekce malwarem

Malware lze klasifikovat jako škodlivý software, jehož záměrem je narušit, poškodit nebo převzít kontrolu nad systémem. Malware se do systému může dostat několika způsoby a samotný uživatel ani nemusí vědět, že k nějaké infekci došlo, instaluje se totiž bez souhlasu uživatele. Hrozí tedy velké riziko, že než se přijde na to, že systém je infikován, malware už způsobí nějaké škody (Stouffer, 2023).

Vnitřní hrozby

Vnitřní hrozby se vztahují především na zaměstnance nebo zkrátka na ty co již mají přístup ke cloudu. Může se jednat o nerespektování pravidel kybernetické bezpečnosti,

jakákoli lhostejnost vůči firemním zásadám a nedbalost. Na druhou stranu ale může jít i o záměrnou škodlivou činnost, jako je sabotáž, krádež dat, poskytnutí přístupu neoprávněným osobám apod. (Stouffer, 2023).

Lidské chyby

Lidské chyby úzce souvisí s vnitřními hrozbami. Ze dříve zmíněných jsou nedbalost a lhostejnost asi takové největší lidské chyby, které mohou vést k narušení dat. Konkrétně se může jednat např. o stažení malwaru z infikovaného softwaru či stránky, používání slabých hesel, kompromitaci IP adresy, odeslání informací špatnému příjemci, neaktualizování softwarů atd. (Stouffer, 2023).

Špatně zabezpečené API

API je rozhraní, které zprostředkovává vzájemnou komunikaci 2 softwarových komponent, aniž by muselo vědět, jak jsou integrovány. Pokud API není dostatečně zabezpečeno může dojít k jeho prolomení, což může dále vést k únikům dat a dalším problémům (Stouffer, 2023).

DoS útoky

Cílem Denial of Service útoku je přetížit zdroje webové stránky a znemožnit tak k dané stránce přístup ostatním uživatelům. Princip DoS útoku spočívá v zahlcení sítě několika tisíci požadavky, do té doby, než dojde k vyřazení sítě z provozu. Následky DoS útoku mohou být zastavení počítačových operací, zadržení dokumentů a souborů případně i přechod zákazníků ke konkurenci (Stouffer, 2023). Kromě DoS útoků existuje riziko tzv. DDoS útoků, které fungují v podstatě na stejném principu, jen jsou prováděny z více počítačů najednou, obvykle z různých lokalit.

Pokročilé přetrvávající hrozby

Jako pokročilé přetrvávající hrozby lze označit neoprávněné dlouhodobé připojení narušitele k síti, za účelem sběru dat či špionáže. Takového narušitele je potom velmi obtížné identifikovat. Terčem pokročilých přetrvávajících hrozeb jsou spíše větší podniky, ale v poslední době se dost často stávají obětmi i malé a střední podniky (Stouffer, 2023).

Další rizika a hrozby

Kromě dříve zmíněných bezpečnostních rizik a hrozeb existuje i řada dalších, jako ztráta dat, nespravovaný prostor pro útok, nedostatečná správa přístupů, shadow IT, útok nultého dne a špatně nakonfigurované cloudové úložiště (Stouffer, 2023).

3.5.3 Zásady správného zabezpečení cloudu

Jedním z takových základních nástrojů, které jsou důležité pro správné zabezpečení systémů cloud computingu je šifrování. Šifrovat lze mimořádně citlivá data, komunikaci s cloudem v plném rozsahu nebo použít tzv. end-to-end šifrování všech dat, která se nahrávají do cloudu. End-to-end neboli koncové šifrování je vhodné zejména pro šifrování vysoce citlivých dat, na druhou stranu, pokud do cloudu nejsou ukládána citlivá data může být koncové šifrování s nadsázkou přehnané. V rámci šifrování je nezbytné dbát na bezpečnou správu šifrovacích klíčů. Mezi takové běžné opatření patří záloha šifrovacích klíčů, kterou je dobré uchovávat, pokud možno mimo cloud. Ideální je také pravidelná výměna šifrovacích klíčů, která zajistí, že pokud by případný útočník zjistil klíč, bude mu po výměně k ničemu (Kaspersky, c2023).

Kromě šifrování je také důležité se řídit základními tipy pro kybernetickou bezpečnost. Takovým nejzákladnějším je používání silných hesel. Ideální je kombinace malých a velkých písmen, číslic a speciálních znaků, přičemž platí, že čím více je řetězec náhodnější, tím je nižší riziko jeho prolomení. Dále je podstatné chránit všechna svá zařízení, která jsou používána pro práci v cloudu, obzvláště pokud je mezi nimi povolena synchronizace dat. Náchylná na krádež či ztrátu jsou speciálně zařízení jako mobilní telefony a tablety, kvůli svým kompaktním rozměrům a neustálé přítomnosti u vlastníka. Dalším doporučením je pravidelné zálohování dat. To funguje jako taková pojistka pro případ, že by došlo k výpadku cloudu či ztrátě dat. Ztracená data lze pak ze zálohy, která je obvykle uchovávána na počítači, pevném disku či dokonce v cloudu velmi snadno obnovit do původní podoby. Doporučováno je rovněž vhodně nastavit uživatelská oprávnění, používat kvalitní antivirový software a pokud možno vyhýbat se přístupu ke svým datům na veřejných Wi-Fi (Kaspersky, c2023).

3.6 Sektor malých a středních podniků

Do sektoru malých a středních podniků spadají podniky s omezeným rozsahem činnosti a omezeným počtem zaměstnanců v porovnání s velkými podniky. Obvykle zahrnuje mikropodniky, malé podniky a střední podniky. Pro zařazení do tohoto sektoru

musí podnik splňovat určité podmínky co se týče počtu zaměstnanců, ročního obratu nebo bilanční sumy roční rozvahy. V případě mikropodniku je maximální počet zaměstnanců stanoven na méně 10, maximální výše ročního obratu nesmí být vyšší než 2 miliony EUR a bilanční suma roční rozvahy taktéž nesmí překročit 2 miliony EUR. Pro malý podnik je charakteristické méně než 50 zaměstnanců a maximální roční výše obratu včetně maximální bilanční sumy roční rozvahy je stanovena na 10 milionů EUR. Střední podnik je charakterizován jako podnik, který zaměstnává méně než 250 zaměstnanců a jehož výše obratu není větší než 50 milionů EUR a jehož bilanční suma roční rozvahy nepřesahuje 43 milionů EUR (BusinessInfo.cz, 2021).

4 Vlastní práce

V této části práce budou nejprve představeni 3 největší poskytovatelé cloudových služeb, kteří budou následně porovnáni na základě předem stanovených kritérií. Dále pak bude vyhotovena vícekriteriální analýza variant a v závěru praktické části bude vyhotoveno doporučení a vyhodnocení získaných výsledků.

4.1 Představení poskytovatelů

Dle společnosti Synergy Research Group (2023) měla největší zastoupení na trhu s cloudovými službami (IaaS, PaaS a hostovaný privátní cloud) ve 3. čtvrtletí v roce 2023 společnost Amazon s celkovým tržním podílem 32 %. V závěsu se držely společnosti Microsoft a Google se svým 23 % a 11 % podílem. Celkový tržní podíl těchto 3 poskytovatelů dohromady činil 66 %, tudíž lze konstatovat, že tito 3 poskytovatelé měli nadpoloviční zastoupení na celosvětovém trhu s cloudovými službami. V případě veřejného cloudu se na trhu Amazon spolu s Microsoftem a Googlem podíleli z 72 %. Nutno dodat, že se nejedná o nedávný trend, nýbrž tito 3 poskytovatelé dominují trh s cloudovými službami již delší dobu.

Pro zpracování praktické části byly záměrně vybráni poskytovatelé veřejného cloudu, jelikož je veřejný cloud často atraktivnější volbou pro malé a střední podniky zejména kvůli nižším vstupním nákladům a snadnější správě, oproti privátnímu cloudu.

4.1.1 Amazon

Společnost Amazon (2024) své cloudové služby pod názvem Amazon Web Services (AWS) spustila poprvé v roce 2006. V dnešní době již nabízí velmi pestrou nabídku služeb se zaměřením na analýzu, integraci aplikací, blockchain, business aplikace, databáze, vývojářské nástroje, Internet of Things (IoT), strojové učení, umělou inteligenci, úložiště a řadu dalších služeb. Sídlo AWS je ve Spojených státech amerických a služby jsou dostupné zákazníkům z celého světa. Aktuální pokrytí v době psaní práce činilo 33 geografických regionů s celkem 105 zónami dostupnosti. Do budoucna Amazon plánuje do svého pokrytí přidat další 4 regiony a 12 zón dostupnosti (Amazon, c2024a).

4.1.2 Microsoft

Cloudová platforma firmy Microsoft s názvem Microsoft Azure byla oproti Amazonu oficiálně spuštěna o několik let později, konkrétně v roce 2010 (Abandy, 2022). Z

rozsáhlého souboru služeb Microsoft Azure nabízí např. služby soustředěné na umělou inteligenci, vývoj aplikací, datové vědy, strojové učení a úložiště. Co se týká pokrytí, Microsoft na svých stránkách uvádí, že pokrývá více než 60 geografických regionů (Microsoft, c2024). Kromě Azure Microsoft provozuje i Microsoft 365, dříve známý pod názvem Office. Jedná se o známou cloudovou platformu, která mimo jiné obsahuje i populární kancelářské aplikace jako Word, Excel, Powerpoint a Outlook.

4.1.3 Google

Google poskytuje své cloudové služby v rámci Google Cloud, a stejně jako u předchozích poskytovatelů je jeho portfolio služeb bohaté, aktuální nabídka činí více než 100 služeb. Některé jsou zaměřené na umělou inteligenci a strojové učení, jiné se soustřeďují např. na analýzu, databáze atd. V nabídce je i Google Workspace, dříve známý jako G Suite. Google (2023a) nezaostává za konkurencí ani v případě pokrytí, v současné době Google Cloud pokrývá 40 geografických regionů.

4.2 Komparativní analýza

Cílem této analýzy bude poskytnout souhrnný přehled o bezpečnostních aspektech u vybraných poskytovatelů cloud computingu. Pro porovnání poskytovatelů byla stanovena tyto kritéria:

1. Standardy, certifikace a právní předpisy
2. Fyzické zabezpečení datových center
3. Šifrování dat v klidu
4. Reakce na bezpečnostní incidenty

Pro stanovení kritérií čerpal autor inspiraci z průzkumu firmy pwc (2019). Data k jednotlivým kritériím byla získána z oficiálních webových stránek a z oficiální dokumentace poskytovatelů.

4.2.1 Kritérium 1. – Standardy, certifikace a právní předpisy

Předmětem tohoto kritéria budou standardy, zákony, regulace, certifikace a další osvědčení, které jednotliví poskytovatelé uvádějí na svých webových stránkách. Kvůli velkému množství bude nejprve u každého poskytovatele uveden celkový počet a poté několik vybraných globálních a evropských standardů. Autor by chtěl rovněž zmínit, že u

jednotlivých poskytovatelů nemusejí být všechny uváděné standardy, certifikace, či právní předpisy v souladu se všemi nabízenými službami.

Amazon

Amazon na svých webových stránkách uvádí, že splňuje 143 standardů, certifikací a právních předpisů. Z ISO/IEC standardů splňuje ISO 9001, ISO 20000, ISO 22301, ISO 27001, ISO 27017, ISO 27701 a ISO 27018. Dále disponuje standardem PCI DSS, který se zaměřuje na bezpečnost dat u platebních karet nebo standardem CSA STAR od Cloud Security Alliance. Rovněž je držitelem certifikací SOC, konkrétně SOC 1, SOC 2 a SOC 3. Velmi důležitý je i soulad s GDPR či CoC (Cloud Code of Conduct), který souvisí s GDPR. Z řady dalších evropských standardů vyhovuje např. německému C5.

Microsoft

Microsoft na rozdíl od Amazonu na svých stránkách neuvádí přesný počet standardů a právních předpisů, které splňuje, ale tvrdí, že jich splňuje více než 100. Proto se autor rozhodl spočítat jednotlivé položky a vyřadit ty, které dle Microsoftu již nejsou splňovány a dospěl k závěru, že Microsoft je v souladu se 104 standardy, certifikacemi či právními předpisy. Z ISO/IEC standardů to jsou ISO 20000, ISO 22301, ISO 27001, ISO 27017, ISO 27018, ISO 27701 a ISO 9001. Z certifikací SOC splňuje všechny, tedy SOC 1, SOC 2 i SOC 3. Plně splňuje i standard CSA STAR a PCI DSS. Co se týče evropských právních předpisů či standardů, Microsoftu nechybí soulad s GDPR, CoC ani s německým C5.

Google

Ani Google na svých webových stránkách neuvádí přesný počet, ale po spočítání autor zjistil, že vyhovuje 167 standardům, certifikacím či právním předpisům. Celkem splňuje 8 ISO/IEC standardů, konkrétně ISO 9001, ISO 27001, ISO 27017, ISO 27018, ISO 22301 (včetně Britské adaptace tohoto standardu), ISO 50001, ISO 27110 a ISO 27701. Vyhovuje i SOC 1, SOC 2, SOC 3 a také CSA STAR a PCI DSS. Z evropských standardů nebo právních předpisů splňuje CoC, C5 a rovněž mu nechybí soulad s GDPR.

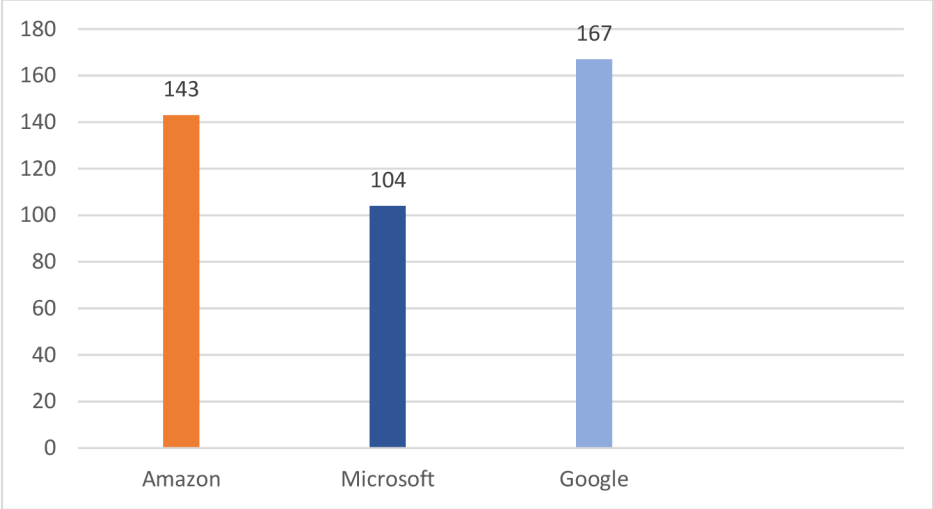
Porovnání

Amazon jako jediný z těchto poskytovatelů má na svých webových stránkách uveden konkrétní počet splňovaných standardů, regulací, právních předpisů či certifikací. Na druhou

stranu ale již neuvádí kompletní seznam, zatímco Microsoft s Googlem naopak uvádějí kompletní seznam splňovaných standardů, ale ne přesný počet. Co se týká počtu, všichni 3 poskytovatelé vyhovují velkému množství standardů, Google je zde však v převaze se 167, následován Amazonem se 143 a Microsoftem se 104 standardy. Tato čísla zahrnují jak globální, tak i regionální standardy, regulace, certifikace či právní předpisy, přičemž ne všechny z nich mají pro podniky stejnou relevanci a rozhodně záleží na tom, v jakém oboru firma podniká a v jakých zemích provozuje svoji činnost.

Dalších odlišností si lze všimnout i ve srovnání z hlediska ISO/IEC standardů. Microsoft s Amazonem se v tomto případě nijak neliší, oba poskytovatelé splňují 7 totožných ISO standardů, ale vyčnívá zde Google, který jich splňuje 8. Odlišná je i skladba standardů, Google splňuje standardy ISO 50001 a ISO 27110, u kterých Amazon s Microsoftem neuvádějí soulad, ale na druhou stranu nesplňuje ISO 20000, se kterým jsou jeho konkurenti v souladu. ISO 50001 je standard, který je zaměřený na praktiky udržitelné energie a hospodaření s energiemi. I přesto, že udržitelná energie je v současnosti velmi důležité téma, tento standard přímo nesouvisí s bezpečnostními aspekty cloud computingu a s bezpečností dat, proto absence souladu Microsoftu a Amazonu s tímto standardem není zásadním problémem. ISO 27110 je už více relevantní co se týká bezpečnosti dat, jedná se o standard, který specifikuje pokyny pro vývoj rámce kybernetické bezpečnosti. Zde by tedy Google mohl mít menší výhodu. Standard ISO 20000 je zaměřený na management IT služeb, jeho absence však nemusí nutně znamenat nedostatek efektivních postupů v managementu IT služeb. ISO 9001, ISO 22301, ISO 27001, ISO 27017, ISO 27701 a ISO 27018 splňují všichni 3 poskytovatelé. Z hlediska cloudové bezpečnosti a všeobecné bezpečnosti dat jsou důležité zejména ISO 27001, ISO 27017, ISO 27018 a ISO 27701. Co se týče certifikací SOC a standardů CSA STAR, PCI DSS a C5, ani jeden z poskytovatelů nezaostává za konkurenty. To samé platí i v případě souladu s GDPR. V následujícím grafu je zobrazeno srovnání poskytovatelů na základě celkového počtu standardů, certifikací či právních předpisů.

Graf 1 Počet standardů, certifikací či právních předpisů



Zdroj: Vlastní zpracování (2024)

4.2.2 Kritérium 2. - Fyzické zabezpečení datových center

Toto kritérium bude zaměřené na fyzické zabezpečení datových center tedy bezpečnostních opatření vnějšku datového centra a bezpečnostních opatření uvnitř samotné budovy datového centra.

Amazon

Amazon poskytuje fyzické zabezpečení datových center ve 4 vrstvách. 1. obvodová vrstva se týká vnějšího zabezpečení. Z vnějšku je areál každého datového centra chráněn vysoce kvalitním oplocením, bezpečnostní stráží a řadou dalších bezpečnostních opatření jako je nepřetržitý kamerový dohled, technologie detekce narušení atd. Pro přístup do datového centra musí jak zaměstnanci, tak i osoby třetí strany projít striktním procesem povolení přístupu. Přístup zaměstnancům je povolen pouze na základě předchozí žádosti s racionálním odůvodněním, kde je mimo jiné specifikováno, k jaké oblasti datového centra potřebuje zaměstnanec přístup a na základě následného přezkoumání dané žádosti speciálně určeným personálem. Tato žádost má časově omezenou platnost a po vypršení platnosti je přístup rázem odvolán. Zaměstnancům, kteří pracují přímo v datovém centru jsou udělena oprávnění pouze k oblastem nezbytným pro vykonávání jejich práce. Tyto zaměstnanci jsou pravidelně kontrolováni speciálně určeným personálem za účelem ověření, zda je jejich oprávnění přístupu nezbytné. Pokud ne, musí projít dříve zmíněným procesem návštěvy. Osoby třetí strany, jak již bylo dříve zmíněno rovněž musí projít striktním procesem

návštěvy. Po povolení přístupu se musí identifikovat průkazem totožnosti a po celou dobu v datovém centru jsou doprovázeny oprávněným personálem (Amazon, c2024d).

Pro vstup do datového centra je nejprve nutné projít vstupní bránou, která je hlídána bezpečnostními pracovníky a je pod dohledem supervizorů (Amazon, c2024e). Samotné vstupní body budovy datového centra jsou také pod kontrolou bezpečnostního personálu a dalších bezpečnostních opatření jako je kamerový systém, systém detekce narušení, bezpečnostní alarmy apod. Podobným způsobem jsou zabezpečeny i serverovny, tedy 2. vrstva. Jakýkoli vstup do budovy datového centru i přístup k jednotlivým oblastem uvnitř datového centra je podmíněn vícefaktorovou autentizací (Amazon, c2024d).

Pro ještě větší úroveň zabezpečení jsou bezpečnostním týmům v rámci datových center k dispozici AWS Security Operations Centers, které podporují zabezpečení datových center nepřetržitými monitorovacími aktivitami a v případě bezpečnostního incidentu či podezření na bezpečnostní incident poskytují analýzu daného incidentu a reagují na něj (Amazon, c2024e).

Co se týká paměťových médií pro ukládání dat uživatelů, tak ta jsou považována jako vysoce citlivá zařízení a je se s nimi nakládáno velmi opatrně po celou dobu jejich životnosti. Média, na kterých byla uchovávána uživatelská data zůstávají pod kontrolou Amazonu do té doby, než proběhne jejich bezpečné vyřazení z provozu (Amazon, c2024d).

3. vrstva se týká infrastruktury datového centra. Z hlediska řádného provozu datových center Amazon provádí pravidelnou preventivní údržbu elektrických a mechanických zařízení s cílem zajistit nepřetržitý provoz. Datová centra jsou také vybavena mechanismy pro řízení klimatu a udržování vhodné provozní teploty v serverovnách s cílem zamezit přehřátí hardwaru. Pro zachování nepřetržitého provozu i v případě nouze je připojení k vodě, elektřině, telekomunikacím a internetu navrženo s redundancí, případně jsou datová centra vybavena záložními zdroji napájení (Amazon, c2024d).

4. environmentální vrstva je věnována opatřením pro kontrolu životního prostředí. Datová centra Amazonu jsou vybavena zařízeními pro automatickou detekci požáru a jeho potlačení a mechanismy pro detekci přítomnosti vody (Amazon, c2024b).

Microsoft

Microsoft má rozdělené fyzické zabezpečení datových center do 6 vrstev. 1. vrstva se týká žádosti o přístup do datového centra a její schválení. Pro vstup do datového centra je nutné mít schválenou žádost o přístup, která je posuzována na základě validního obchodního

zdůvodnění. Žádosti jsou posuzovány zaměstnanci Microsoftu a při jejich posuzování se bere v potaz, zda je opravdu nezbytná přítomnost dané osoby v datovém centru s cílem udržet počet osob v datovém centru na minimum. V případě vyhovění žádosti má daná osoba přístup pouze k předem schválené oblasti, a to na omezenou dobu. Po vypršení platnosti oprávnění k přístupu okamžitě zaniká (Microsoft, 2023a).

2. vrstva je zaměřena na přístup návštěvníků. Pro přístup do datového centra musí mít návštěvníci nejprve schválenou žádost a po příchodu obdrží dočasnou přístupovou kartu s označením "Escort Only". Návštěvníci se nemohou nikde pohybovat sami, musí se vždy držet v bezprostřední blízkosti svého doprovodu. Rovněž nemají žádné povolení k přístupu tzn., že se mohou pohybovat pouze v oblastech, ke kterým má doprovod přístup. Při odchodu je nutné, aby návštěva vrátila zpět dočasnou přístupovou kartu. Pro kontrolu je vždy na začátku a na konci každé směny prováděna inventarizace přístupových karet (Microsoft, 2023a).

3. vrstva, vnější zabezpečení datového centra se skládá z vysokého oplocení z oceli a betonu, nepřetržitého kamerového dohledu, bezpečnostních hlídek a dalších bezpečnostních opatření. Vstup a odchod z areálu datového centra je možný pouze vyhrazenými prostory (Microsoft, 2023a).

4. vrstva, tedy vstup do budovy datového centra je pod neustálým kamerovým dohledem a je možný pouze přes bezpečnostní personál (Microsoft, 2023a).

Po vstupu do budovy bezprostředně následuje 5. vrstva. Pro další pohyb v datovém centru je nezbytné projít dvoufaktorovou autentizací s biometrickými údaji. Po ověření identity je povolen přístup pouze k předem schválené oblasti po předem sjednanou dobu (Microsoft, 2023a).

6. vrstva se týká už samotných místností se servery. Přístup i odchod je zde podmíněn mimo jiné kontrolou na přítomnost kovů a vstup je možný pouze se schválenými zařízeními (Microsoft, 2023a).

K likvidaci zařízení Microsoft přistupuje na základě osvědčených postupů, kdy po skončení životnosti je zařízení zlikvidováno s důrazem na bezpečí obsažených dat. Pevné disky jsou buďto bezpečně vymazány nebo zničeny (Microsoft, 2023a).

Neustálý provoz datových center zajišťují nepřerušitelné zdroje napájení, nouzové generátory a palivové rezervy v každém datovém centru (Microsoft, 2023b).

Pro zvýšení zabezpečení Microsoft také provozuje svá bezpečnostní operační střediska, která pomáhají s monitorováním datových center a aktivně se zapojují do řešení případných bezpečnostních incidentů (Microsoft, 2023b).

Google

Fyzické zabezpečení datových center Googlu zahrnuje rovněž 6 vrstev. Mezi opatření týkající se 1. a 2. vrstvy, tedy vnějšku datového centra spadá chytré oplocení s technologií, která je schopna detekovat, zda se nachází někdo poblíž nebo se oplocení přímo dotýká, bezpečnostní stráž, termální a standardní kamery, technologie detekce narušení, nárazové bariéry schopné zastavit plně naložený nákladní automobil apod. Přes vstupní bránu jsou puštěni pouze ověření zaměstnanci. Bezpečnostní pracovníci mají přehled o každé osobě po celou dobu jejího setrvání v datovém centru či jeho areálu (Google Cloud Tech, 2020).

3. vrstva se už týká samotného vstupu do datového centra, kdy je nejprve potřeba projít tzv. secure lobby, kde je nezbytné se prokázat vícefaktorovou autentizací, konkrétně čipovou kartou a absolvovat sken oční duhovky. Vícefaktorovou autentizací je rovněž podmíněn každý vstup uvnitř datového centra a pro větší bezpečnost dveřmi může projít současně pouze 1 osoba (Google Cloud Tech, 2020).

4. vrstva zahrnuje provozní místnosti jako místnost páteřní sítě a místní bezpečnostní operační středisko. To je v podstatě základnou celého bezpečnostního systému. Průchody dveřmi, kamery, oplocení, skeny duhovky atd., to vše je monitorováno v bezpečnostním operačním středisku. Google má kromě místních bezpečnostních středisek také regionální (Google Cloud Tech, 2020).

5. vrstva už jsou samotné servery. Do serveroven mají přístup pouze zaměstnanci, kteří mají na starost údržbu, vylepšení či opravy příslušných zařízení. Zaměstnanci však nemají přístup k datům na těchto zařízeních díky šifrování (Google Cloud Tech, 2020).

V 6. vrstvě probíhá destrukce paměťových médií. Výkon paměťových médií je pravidelně testován, pokud výkon neodpovídá požadavkům, je disk navržen na vyřazení. Disky určené k vyřazení jsou předány pomocí bezpečné dvoucestné skříňky technikům, kteří mají speciální povolení pro přístup do místnosti, kde se provádí samotná destrukce disků. Poté je obsah paměťového média vymazán a následně je disk zničen. Při odchodu ze 6. a 5. vrstvy musí zaměstnanci podstoupit kontrolu na přítomnost kovů pod dohledem bezpečnostního personálu (Google Cloud Tech, 2020).

Pro nepřetržitý provoz datových center jsou energetické systémy navrženy s redundancí a každá kritická komponenta má primární a alternativní zdroj energie. Pro snížení pravděpodobnosti výpadku a poškození hardwaru jsou datová centra také vybavena chladícími systémy a zařízeními pro detekci a potlačení požáru (Google, 2023b).

Google také pravidelně testuje celkové zabezpečení datových center. Pro testování vnějšího zabezpečení si najímá specializované firmy a pro testování zabezpečení uvnitř centra jsou zaměstnanci pověřeny Googlem, aby na zkoušku porušili bezpečnostní protokoly (Google Cloud Tech, 2020).

Dalším přidaným bezpečnostním prvkem jsou na zakázku vyrobené servery a síťové vybavení přímo pro potřeby datových center, z nichž některé jsou navrženy přímo Googlem (Google, 2023b).

Porovnání

Microsoft a Google mají rozdělené fyzické zabezpečení datových center do 6 vrstev, zatímco Amazon své zabezpečení člení do 4 vrstev, přičemž se poskytovatelé liší v zaměření jednotlivých vrstev. Co se týká vnějšího zabezpečení datových center, tak každý z poskytovatelů má areál datového centra pod nepřetržitým kamerovým dohledem a v areálu je neustále přítomna bezpečnostní stráž. Poskytovatelé také používají technologie detekce narušení a areál mají ohraničený kvalitním oplocením. Oplocení Googlu je navíc obohaceno o další technologie pro detekci narušení. Google má také u hlavní příjezdové brány datového centra nainstalované nárazové bariéry.

K povolení vstupu do datového centra Amazon a Microsoft přistupují velmi podobným způsobem, kdy je nejprve třeba podat žádost s obchodním odůvodněním a poté je tato žádost vyhodnocena specializovaným personálem a v případě povolení se daná osoba může zdržovat pouze v předem schválené oblasti, a to do vypršení platnosti daného povolení. V případě návštěv navíc oba poskytovatelé vyžadují neustálou přítomnost doprovodu. Google neuvádí přesný postup, kterým se řídí při povolování vstupu do datového centra, ale jednoznačně vymezuje, že do datového centra mohou zavítat pouze ověření zaměstnanci. U všech 3 poskytovatelů je při vstupu do areálu datového centra nutné nejprve projít vstupní bránou. Liší se ale v samotném vstupu do budovy, kdy Amazon vyžaduje identifikaci vícefaktorovou autentizací za přítomnosti bezpečnostního personálu při vstupu do budovy, zatímco Google vyžaduje vícefaktorovou autentizaci až po vstupu do budovy v tzv. secure lobby, rovněž za přítomnosti bezpečnostních pracovníků. Vstup do budovy datového centra

Microsoftu je také hlídán bezpečnostní stráží a vícefaktorová autentizace je vyžadována až po vstupu do budovy a je podmínkou pro další pohyb uvnitř datového centra. To mají všichni 3 poskytovatelé společné, v rámci přístupu k různým oblastem datového centra je třeba se prokázat vícefaktorovou autentizací. Zejména při vstupu do místností se servery, které jsou v případě Amazonu chráněny systémy detekce narušení, kamerovým systémem, bezpečnostními alarmy a vstoupit mohou pouze oprávněné osoby. Do místností se servery Googlu a Microsoftu také mohou vstoupit pouze oprávnění zaměstnanci, ale Microsoft navíc vyžaduje kontrolu na přítomnost kovů, kterou je nutné absolvovat před vstupem i po odchodu ze serveroven. Google vyžaduje kontrolu na přítomnost kovů pouze při odchodu z místností se servery.

K destrukci paměťových médií přistupují všichni 3 poskytovatelé zodpovědně s důrazem na bezpečnost obsažených dat. Google však uvádí podrobnější postup popsaný již dříve, který zahrnuje dvoucestné skříňky a místnost, kde probíhá samotná destrukce.

Všichni 3 poskytovatelé se snaží udržet nepřerušovaný chod svých datových center, Amazon má datová centra koncipována s redundantním připojením k vodě, elektřině, telekomunikacím a internetu včetně záložních zdrojů napájení. Dále pak využívá mechanismy pro řízení klimatu a udržování vhodné provozní teploty a mechanismy pro detekci přítomnosti vody, včetně zařízení pro detekci a potlačení požáru, aby zamezil poškození hardwaru. Energetické systémy datových center Googlu jsou rovněž navrženy s redundancí, plus má každá kritická komponenta zajištěna alternativní zdroj energie. Jako ochranu před poškozením hardwaru Google využívá chladící systémy a stejně jako Amazon zařízení pro detekci a potlačení požáru. Microsoft pouze zmiňuje, že pro nepřetržitý chod datových center využívá nepřerušitelné zdroje napájení včetně nouzových generátorů a palivových rezerv.

Bezpečnostní operační střediska, která podporují zabezpečení datových center mají implementována všichni 3 poskytovatelé.

Google od svých konkurentů vyčnívá tím, že si nechává na zakázku vyrobit servery a síťové vybavení, z nichž některé sám navrhuje, přímo pro potřeby datových center. Dále pak také provádí testování vnějšího a vnitřního zabezpečení datových center.

4.2.3 Kritérium 3. – Šifrování dat v klidu

Toto kritérium bude zaměřené na možnosti šifrování v klidu, správu šifrovacích klíčů, podporované služby, výchozí nastavení a na algoritmus použitý při šifrování. Pro názornější

porovnání bude u každého poskytovatele sestavena tabulka a v porovnání bude vytvořena souhrnná tabulka z jednotlivých dílčích tabulek.

Amazon

Šifrování v klidu je podporováno u všech služeb, které jsou poskytovány Amazonem. Neznamená to však, že data jsou ve všech službách šifrována automaticky. Šifrování v klidu ve výchozím nastavení nabízí třeba služba Amazon S3. Na úrovni hardwaru jsou samozřejmě všechna data šifrována. Amazon umožňuje jak client-side, tak i server-side šifrování. U Client-side šifrování zašifrování dat probíhá předtím, než byla nahrána do cloudu. Při použití tohoto způsobu je správa šifrování v režii uživatelů tzn., že si uživatelé spravují šifrovací klíče sami, ale mohou také pro správu klíčů využít AWS Key Management Service (KMS). Pro client-side šifrování lze i využít služby přímo od Amazonu jako třeba S3 Encryption Client. Server-side šifrování znamená, že data jsou zašifrována při uložení na server. Amazon nabízí 3 možnosti server-side šifrování: SSE with customer provided encryption keys (SSE-C), SSE with Amazon S3 managed encryption keys (SSE-S3) a SSE with AWS KMS stored encryption keys (SSE-KMS). SSE-C neboli server-side šifrování se šifrovacími klíči poskytnutými uživatelem v podstatě znamená, že uživatel si sám spravuje šifrovací klíče, přičemž Amazon se stará o šifrování a dešifrování. Tuto možnost však nepodporují všechny služby Amazonu. SSE-S3 znamená server-side šifrování se šifrovacími klíči pod správou Amazon S3. Tato možnost je nastavena jako výchozí šifrování ve službě Amazon S3. SSE-KMS je server-side šifrování s klíči uloženými v AWS KMS. KMS je služba od Amazonu, která usnadňuje správu šifrovacích klíčů. Klíče mohou být spravované buďto Amazonem nebo uživatelem. Uživatelé tedy mohou spravovat (vytvářet, mazat apod.) pouze uživatelem spravované klíče. Klíče, které jsou pod správou Amazonu si mohou pouze zobrazit, ale nemohou s nimi provádět žádné operace. Pro šifrování Amazon používá AES-256 (Perry, 2022). Pro větší názornost byly veškeré informace shrnuty do následující tabulky.

Tabulka 1 Přehled o šifrování v klidu – Amazon

Šifrování v klidu	**Amazon**
Podporované služby	Všechny služby
Šifrování ve výchozím nastavení	Ne všechny služby
Client-side	Ano
Server-side	1. SSE with customer provided encryption keys (SSE-C) 2. SSE with Amazon S3 managed encryption keys (SSE-S3) 3. SSE with AWS KMS stored encryption keys (SSE-KMS)
Správa klíčů	AWS Key Management Service (KMS)
Algoritmus	AES-256

Zdroj: Vlastní zpracování (2024)

Microsoft

Microsoft také umožňuje šifrování v klidu u všech nabízených služeb. Ve výchozím nastavení však mají nastavené šifrování v klidu pouze některé služby jako třeba Azure Storage, přičemž na úrovni hardwaru jsou šifrována všechna data. Microsoft rovněž umožňuje client-side a server-side šifrování. U client-side šifrování mají uživatelé úplnou kontrolu nad svými klíči. U server-side šifrování Microsoft nabízí 3 možnosti: Service-managed keys v překladu klíče spravované službou, Customer-managed keys neboli klíče spravované uživatelem a Customer-managed keys in customer-controlled hardware tedy klíče spravované zákazníkem v zákazníkem řízeném hardwaru. První z možností znamená, že šifrování a správa klíčů je v režii Microsoftu. Customer-managed keys umožňuje uživatelům spravovat ve službě Azure Key Vault buďto své klíče nebo klíče nově generované. Třetí z možností v podstatě znamená, že uživatelé používají vlastní šifrovací klíče, jež jsou uložené mimo kontrolu Microsoftu. Kvůli komplikovanější konfiguraci tato možnost není podporována ve většině služeb. Služba Azure Key Vault je v podstatě úložiště šifrovacích klíčů, kde uživatelé mohou vytvářet či spravovat šifrovací klíče. Jedná se o obdobu AWS KMS. Pro šifrování Microsoft také používá AES-256 (Microsoft, 2024a). Tabulka 2 obsahuje shrnutí informací o šifrování v klidu Microsoftu.

Tabulka 2 Přehled o šifrování v klidu – Microsoft

Šifrování v klidu	**Microsoft**
Podporované služby	Všechny služby
Šifrování ve výchozím nastavení	Ne všechny služby
Client-side	Ano
Server-side	1. Service-managed keys 2. Customer-managed keys 3. Customer-managed keys in customer-controlled hardware
Správa klíčů	Azure Key Vault
Algoritmus	AES-256

Zdroj: Vlastní zpracování (2024)

Google

Stejně jako konkurence Google podporuje šifrování v klidu u všech svých služeb. Výjimkou je však šifrování ve výchozím nastavení u všech služeb, tedy veškerá data nahraná uživatelem jsou automaticky šifrována. To samozřejmě platí i na hardwarové úrovni. Google rovněž podporuje client-side i server-side šifrování. Díky server-side šifrování ve výchozím nastavení jsou navíc data uživatelů, kteří využívají client-side šifrování zašifrována ještě jednou (Google, 2022b). Kromě výchozího server-side šifrování, kdy se o správu klíčů a šifrování stará Google, je možné využít další 2 možnosti: Customer-managed keys a Customer-supplied keys. Customer-managed keyes v překladu uživatelem spravované klíče umožňují uživatelům vytvářet a spravovat šifrovací klíče prostřednictvím služby Cloud Key Management Service. Customer-supplied keys neboli uživatelem dodané klíče dávají možnost uživatelům dodat a spravovat vlastní šifrovací klíče. Služba pro správu šifrovacích klíčů Cloud KMS je analogií AWS KMS a Azure Key Vault. Google stejně jako Amazon a Microsoft pro šifrování používá AES-256 (Google, 2024). Veškeré informace o šifrování v klidu Googlu byly shrnuty do následující tabulky.

Tabulka 3 Přehled o šifrování v klidu – Google

Šifrování v klidu	**Google**
Podporované služby	Všechny služby
Šifrování ve výchozím nastavení	Všechny služby
Client-side	Ano
Server-side	1. Default encryption 2. Customer-managed keys 3. Customer-supplied keys
Správa klíčů	Cloud Key Management Service (KMS)
Algoritmus	AES-256

Zdroj: Vlastní zpracování (2024)

Porovnání

Tabulka 4 obsahuje porovnání poskytovatelů z hlediska šifrování v klidu.

Tabulka 4 Porovnání poskytovatelů

Šifrování v klidu	**Amazon**	**Microsoft**	**Google**
Podporované služby	Všechny služby	Všechny služby	Všechny služby
Šifrování ve výchozím nastavení	Ne všechny služby	Ne všechny služby	Všechny služby
Client-side	Ano	Ano	Ano
Server-side	1. SSE with customer provided encryption keys (SSE-C) 2. SSE with Amazon S3 managed encryption keys (SSE-S3) 3. SSE with AWS KMS stored encryption keys (SSE-KMS)	1. Service-managed keys 2. Customer-managed keys 3. Customer-managed keys in customer-controlled hardware	1. Default encryption 2. Customer-managed keys 3. Customer-supplied keys
Správa klíčů	AWS Key Management Service (KMS)	Azure Key Vault	Cloud Key Management Service (KMS)
Algoritmus	AES-256	AES-256	AES-256

Zdroj: Vlastní zpracování (2024)

4.2.4 Kritérium 4. - Reakce na bezpečnostní incidenty

Toto kritérium se bude zabývat postupem, kterým jednotlivý poskytovatelé reagují na bezpečnostní incidenty a také jak se poskytovatelé staví k oznamování bezpečnostních incidentů.

Amazon

V případě, že dojde k nějakému bezpečnostnímu incidentu Amazon bez prodleně oznámí tuto skutečnost uživateli a okamžitě reaguje na daný incident přijetím vhodných opatření ke zmírnění či eliminaci nepříznivých následků. V oznámení o incidentu Amazon uživatelům sděluje pouze informace, které může sdělit s přihlédnutím na různá omezení. Amazon uživatelům však neoznamuje tzv. neúspěšné bezpečnostní incidenty. To jsou bezpečnostní incidenty, při kterých nedošlo k neoprávněnému přístupu k datům uživatelů či k zařízení Amazonu, na kterých jsou uchovávána uživatelská data. Příkladem mohou být útoky na firewall, neúspěšné pokusy o přihlášení, DoS útoky apod. Oznámení o bezpečnostním incidentu Amazon doručuje uživatelům způsobem, kterým uzná za vhodný, včetně e-mailu (Amazon, 2023).

Proces reakce Amazonu na bezpečnostní incidenty se skládá ze 3 fází. První fáze je Aktivace a oznámení. Zde spadá detekce událostí, nejčastěji prostřednictvím metrik či alarmů, které jsou v provozu nepřetržitě po celý rok, dále pak pomocí problémových tiketů zadaných zaměstnancem či prostřednictvím volání uživatelů na linku technické podpory. Pokud detekovaná událost splňuje kritéria bezpečnostního incidentu, tak je prostřednictvím nástrojů pro správu událostí zahájeno řešení daného incidentu a do řešení jsou zapojeni příslušný pracovníci, kteří provedou analýzu incidentu s cílem zjistit hlavní příčinu. Ve 2. fázi Obnova je daný incident opraven příslušnými pracovníky a po vyřešení dalších souvisejících problémů jsou stanoveny další kroky týkající se dokumentace a následného postupu. Po dokončení fáze obnovy následuje fáze Rekonstituce, kdy příslušný tým zaměstnanců provede post mortem analýzu a hloubkovou analýzu příčiny incidentu. Výsledky post mortem analýzy jsou pak následně předloženy vrcholovému managementu, jímž jsou přezkoumány a případná opatření jsou zaznamenána do dokumentu o opravě chyb (COE) (Amazon, c2024c).

Amazon také provádí pravidelné testování procesu reakce na incidenty. Cílem tohoto testování je odhalení případných závad a připravení zaměstnanců na zvládání incidentů. Toto testování Amazon provádí každoročně a předmětem testování jsou různorodé scénáře,

potenciální vektory útoku, zapojení systémového integrátora do hlášení a koordinace nebo různé způsoby hlášení či detekce (od uživatelů, od zaměstnanců). Výsledky testování jsou pak prověřovány audity třetí stranou (Amazon, 2019).

Microsoft

Oznámení o bezpečnostním incidentu Microsoft sděluje uživatelům nejpozději do 72 hodin od zaznamenání incidentu. Výjimkou může být např. když se Microsoft domnívá, že oznámení by mohlo upozornit nežádoucího uživatele a vystavit tak další uživatele bezpečnostním rizikům, nebo pokud nejsou do 72 hodin všechny detaily o bezpečnostním incidentu k dispozici. V oznámení jsou uvedeny podrobné informace týkající se bezpečnostního incidentu s cílem usnadnit uživatelům interní šetření. Oznámení Microsoft uživatelům doručuje prostřednictvím portálu Service Health, v odůvodněných případech e-mailem (Microsoft, 2024b).

Proces reakce na bezpečnostní incidenty Microsoftu se skládá z 5 fází. První fází je Detekce. Ta probíhá např. pomocí automatizovaných systémových upozornění pocházejících z alarmů, detekcí neoprávněných vniknutí či algoritmů pro detekci anomálií, dále pak prostřednictvím oznámení od zákazníků v portálu zákaznické podpory nebo upozorněním na událost zaměstnanci Microsoftu. Druhou fází je Posouzení, kdy pracovník z týmu reakce na incidenty posoudí dopad a závažnost události. Na základě posouzení je pak dále rozhodnuto, zda je zapotřebí asistence dalšího týmu při řešení události. Ve 3. fázi Diagnóza jsou experty na reakce na incidenty provedena technická nebo forenzní vyšetřování a identifikovány strategie omezení a mitigace. V této fázi je uskutečněno i oznámení o incidentu zákazníkům v případě podezření na únik uživatelských dat. 4. fáze Stabilizace a zotavení se týká vytvoření plánu obnovy, přijetí opatření ke zmírnění krize či naplánování dlouhodobějších zmírňujících opatření. Finální fází je Uzavření incidentu a post-mortem. V této fázi je týmem zaměřeným na reakce na incidenty vypracována post-mortem analýza s detaily incidentu, na jejímž základě jsou pak revidovány zásady, postupy a procesy s cílem zabránit opakování stejného nebo podobného incidentu (Microsoft, 2024b).

Microsoft navíc každoročně pořádá tréninky pro různá interní oddělení s cílem připravit je na skutečné incidenty. Součástí tohoto tréninku jsou cvičení se zástupci z týmu pro reakce na incidenty, bezpečnostního týmu, právních týmů a komunikačního týmu. Výsledky cvičení jsou dokumentovány včetně případných metod nápravy. Kromě tréninků

Microsoft také vyžaduje po příslušných zaměstnancích absolvovat školení zaměřené na základy ochrany osobních údajů, nařízení GDPR a osvědčených postupů, co se týče identifikace a hlášení incidentů. Pro veškerý personál je navíc povinné pravidelné školení (Microsoft, 2023c).

Google

Google informuje uživatele o bezpečnostních incidentech v případě, že vydání oznámení nevystaví uživatele bezpečnostním rizikům. Oznámení jsou vydávána co nejrychleji a obsahují podrobné a klíčové informace o incidentu, kroky, které Google podnikl ke zmírnění možných rizik a návrh opatření, dle kterého se mohou uživatelé řídit při řešení incidentu. Neoznamují se však neúspěšné pokusy o přihlášení, skenování portů, DoS útoky, útoky na firewall, zkrátka hrozby, při kterých nedošlo k ohrožení či nějakému narušení uživatelských dat (Google, 2022a).

Google se v případě bezpečnostního incidentu řídí procesem, který má 5 fází. Cílem první fáze Identifikace je detekce a nahlášení bezpečnostních incidentů prostřednictvím automatizovaných nebo manuálních procesů, jako jsou např. různé formy testování, interní revize kódu, nahlášení zaměstnancem nebo automatická analýza síťových a systémových logů. Druhá fáze je Koordinace. V této fázi odpovědný pracovník přezkoumá a provede vyhodnocení hlášení o incidentu a případně zahájí proces reakce na incident, kdy je nejprve pohotově jmenován velitel incidentu neboli osoba, která koordinuje reakce na incident a jeho řešení. Poté co je incident posouzen velitelem incidentu se provedou případné úpravy závažnosti incidentu a do řešení je zapojen tým pro reakce na incidenty, jehož vedoucí jsou určeny velitelem incidentu. Ten stanoví vedoucího pracovníka pro produkt a pro právní záležitosti a přidělí odpovědnost za vyšetřování. Způsob reakce na incident je pak z části ovlivněn posouzením závažnosti, které je založeno na klíčových faktech, jež byly shromážděny a analyzovány týmem pro reakci na incident. Těmi mohou být třeba stav incidentu, dopad na funkčnost poskytovaných služeb nebo typ dat, která mohla být kompromitována. Tyto zásadní skutečnosti jsou pravidelně přehodnocovány na základě vývoje informací za účelem zajištění adekvátní reakce. 3. fáze Usnesení se týká zkoumání hlavní příčiny incidentu a snížení jeho dopadu včetně eliminace případných bezprostředních bezpečnostních rizik a nápravy a obnovy zasažených systémů, dat či služeb. K vyřešení incidentu jsou podniknuty patřičné kroky, jako třeba technické nebo forenzní vyšetřování. V této fázi také probíhá komunikace s uživateli. Ve 4. fázi Uzavření incidentu je týmem pro

reakce na incident provedeno vyhodnocení zkušeností získaných z incidentu. Případně je velitelem incidentu navrhnuto vypracování post-mortem analýzy, kde jsou přezkoumány příčiny incidentu, reakce na daný incident a jsou určeny klíčové oblasti pro zlepšení. V případě nutnosti je vypracován i akční plán. Samotný incident je uzavřen po dokončení nápravných prací. Poslední fáze je Neustále zlepšování. Tato fáze spočívá v neustálém zlepšování procesu reakce na incidenty na základě získaných zkušeností při řešení incidentů, pravidelného školení zaměstnanců, vylepšování nástrojů a také testování procesů a postupů reakce na incidenty (Google, 2022a).

Porovnání

V tabulce 5 jsou poskytovatelé porovnáni na základě kritéria Reakce na bezpečnostní incidenty.

Tabulka 5 Porovnání poskytovatelů

Proces reakce na bezpečnostní incidenty	Amazon	Microsoft	Google
1. fáze	Aktivace a oznámení	Detekce	Identifikace
2. fáze	Obnova	Posouzení	Koordinace
3. fáze	Rekonstituce	Diagnóza	Usnesení
4. fáze	-	Stabilizace a zotavení	Uzavření incidentu
5. fáze	-	Uzavření incidentu a post-mortem	Neustálé zlepšování

Zdroj: Vlastní zpracování (2024)

4.3 Vícekriteriální analýza variant

Cílem této analýzy bude seřazení variant, tedy vybraných poskytovatelů cloudových služeb na základě kritérií z komparativní analýzy. Pro stanovení vah kritérií i pro následné uspořádání jednotlivých variant bude vzhledem k povaze kritérií použita metoda pořadí.

4.3.1 Stanovení vah kritérií

Váhy jednotlivých kritérií budou stanoveny pomocí metody pořadí, která spočívá v uspořádání kritérií dle preference a následném přidělení bodů sestupně dle pořadí. Nejdůležitějšímu kritériu je přiřazen počet bodů rovný počtu kritérií a každé další kritérium v pořadí musí mít o bod méně než předchozí. V případě rovnocennosti kritérií je daným kritériím uděleno bodové ohodnocení dle průměrného pořadí. Po udělení bodů se body

sečtou a tímto součtem se každé přidělené bodové ohodnocení vydělí, čímž se získá váha kritérií. Suma takto získaných vah musí být 1 (100 %).

Kritéria z předchozí komparativní analýzy byla seřazena v následujícím pořadí: Fyzické zabezpečení datových center, Šifrování v klidu, Reakce na bezpečnostní incidenty a Standardy certifikace či právní předpisy. Je důležité zdůraznit, že metoda pořadí je subjektivní a vybrané pořadí bylo zvoleno na základě autorova úsudku, tzn. že nemusí přesně odrážet objektivní hodnotu jednotlivých kritérií. Vypočtené váhy kritérií jsou uvedeny v tabulce 6.

Tabulka 6 Stanovení vah metodou pořadí

Kritéria	**Pořadí**	**Body**	**Váhy**
Standardy certifikace či právní předpisy	4.	1	0,1
Fyzické zabezpečení datových center	1.	4	0,4
Šifrování v klidu	2.	3	0,3
Reakce na bezpečnostní incidenty	3.	2	0,2

Zdroj: Vlastní zpracování (2024)

4.3.2 Seřazení jednotlivých variant

Pro uspořádání variant bude použita metoda pořadí s váhami. Podobně jako u stanovení vah, při výběru kompromisní varianty či seřazení variant je nutné určit pořadí. Určuje se však pořadí variant, a to pro každé kritérium zvlášť. Následně se pak variantám udělí body na základě pořadí stejným způsobem, jako při stanovení vah. Celkové bodové ohodnocení se vypočítá jako skalární součin bodů variant u jednotlivých kritérií s dílčími váhami kritérií. Výsledné seřazení variant či kompromisní varianta se pak určí na základě celkového bodového ohodnocení.

V následující tabulce bude znázorněno autorem stanovené pořadí variant u každého kritéria. Pořadí variant bylo zvoleno na základě komparativní analýzy.

Tabulka 7 Pořadí variant

Kritéria	Varianty		
	Amazon	Microsoft	Google
Standardy certifikace či právní předpisy	2.	3.	1.
Fyzické zabezpečení datových center	2.	2.	2.
Šifrování v klidu	2,5.	2,5.	1.
Reakce na bezpečnostní incidenty	2.	1.	3.

Zdroj: Vlastní zpracování (2024)

Na základě zvoleného pořadí pak byly jednotlivým variantám přiděleny body sestupně dle pořadí. Celkové ohodnocení bylo vypočteno skalárním součinem bodů variant s váhami a na jeho základě bylo stanoveno výsledné pořadí variant. V následující tabulce je uvedeno finální pořadí.

Tabulka 8 Seřazení variant

Kritéria	Varianty			Váhy
	Amazon	Microsoft	Google	
Standardy certifikace či právní předpisy	2	1	3	0,1
Fyzické zabezpečení datových center	2	2	2	0,4
Šifrování v klidu	1,5	1,5	3	0,3
Reakce na bezpečnostní incidenty	2	3	1	0,2
Celkové ohodnocení	**1,85**	**1,95**	**2,2**	
Výsledné pořadí	**3.**	**2.**	**1.**	

Zdroj: Vlastní zpracování (2024)

5 Výsledky

Komparativní analýza obsahuje souhrnný přehled o standardech, certifikacích či právních předpisech, fyzickém zabezpečení datových center, šifrování v klidu a reakci na bezpečnostní incidenty v Amazonu, Microsoftu a Googlu včetně jejich vzájemného porovnání. Tento přehled by mohl malým a středním podnikům pomoci rozhodnout se při výběru poskytovatele cloudových služeb nebo přinejmenším poskytnout strukturované informace o bezpečnostních aspektech jednotlivých poskytovatelů. Vyhotovená komparativní analýza byla použita jako podklad pro vypracování vícekriteriální analýzy variant.

Vícekriteriální analýzou variant byly poskytovatelé seřazeni v následujícím pořadí: Google, Microsoft a Amazon s hodnotami 2,2, 1,95 a 1,85. Na základě těchto výsledků lze usoudit, že co se týče zabezpečení, Google vyšel jako nejlepší varianta a Amazon jako nejméně vhodná varianta. Rozhodujícím faktorem bylo šifrování v klidu ve výchozím nastavení u všech služeb.

5.1 Doporučení

Při volbě poskytovatele cloudových služeb z hlediska bezpečnosti by autor doporučil malým a středním podnikům zaměřit se zejména na kritéria, která byla zkoumána v rámci této bakalářské práce, tedy Standardy, certifikace či právní předpisy, Fyzické zabezpečení datových center, Šifrování v klidu a Reakce na bezpečnostní incidenty. Na základě těchto kritérií si lze vytvořit ucelenou představu o bezpečnostních aspektech poskytovatele cloudových služeb.

Ze standardů jsou důležité zejména standardy z rodiny ISO 27000, které jsou zaměřené na informační bezpečnost nebo certifikace CSA STAR. Doslova nezbytný je soulad poskytovatele s GDPR. Dále je také důležité si ověřit, zda u některých poskytovatelem uváděných standardů již nevypršela platnost.

V případě fyzického zabezpečení datových center je podstatné vědět, zda má ke klíčovým oblastem datového centra přístup pouze autorizovaný personál, jaké poskytovatel používá přístupové kontroly, zda má dostatečně kvalitní kamerový systém a systémy detekce požáru a zda má záložní zdroje energie pro případ výpadků elektřiny. Špatné zabezpečení datových center představuje příliš velké riziko ztráty citlivých dat, což může nejenom poškodit pověst podniku, ale také vést k vysokým pokutám a právním následkům.

Dále je při výběru poskytovatele nezbytné si zjistit, zdali poskytovatel umožňuje šifrování v klidu a pro kolik služeb, jestli umožňuje client-side i server-side šifrování a jejich možnosti, jaké používá šifrovací algoritmy a jaké nabízí možnosti správy šifrovacích klíčů.

Co se týká reakce na bezpečnostní incidenty, klíčová je zejména schopnost poskytovatele rychle reagovat. S tím se pojí aktivní monitorování bezpečnostních hrozeb, pravidelná školení personálu a testování reakce na simulovaných incidentech. Dále je dobré vědět, jak se poskytovatel staví ke sdílení informací a jakým způsobem se vypořádává s incidenty.

Každý z porovnávaných poskytovatelů má velmi kvalitní zabezpečení, ale na základě výsledků vícekriteriální analýzy variant by autor pro malé a střední podniky doporučil Google.

6 Závěr

Tato bakalářská práce byla rozdělena do dvou částí. Cílem teoretické části bylo definovat cloud computing, popsat jeho historii a základní charakteristiky, modely cloud computingu a cloudovou bezpečnost. Cílem praktické části byla analýza a porovnání tří největších poskytovatelů cloudových služeb z hlediska bezpečnosti. Dalším cílem praktické části bylo vytvoření přehledu o bezpečnostních aspektech vybraných poskytovatelů.

V teoretické části byly nejprve uvedeny tři definice cloud computingu, pět základních charakteristik a stručný popis historie cloud computingu. Dále byly popsány čtyři modely nasazení a ke každému byly uvedeny výhody a nevýhody. Autor dále charakterizoval tři hlavní distribuční modely s výhodami a nevýhodami a rovněž se zmínil o několika méně známých distribučních modelech. Poté se teoretická část zaměřila na popis tří komponentů cloudu. Dále následovala kapitola Bezpečnost, ve které byla vysvětlena cloudová bezpečnost a v rámci podkapitol bylo definováno pět základních kategorií cloudového zabezpečení, vymezeno několik významných bezpečnostních rizik a hrozeb a kapitolu uzavíraly klíčové zásady správného zabezpečení cloudu. Na závěr teoretické části autor definoval podniky spadající do sektoru malých a středních podniků, tedy mikropodniky a malé a střední podniky.

V úvodu praktické části byli představeni a stručně charakterizováni tři největší poskytovatelé cloudových služeb: Amazon, Microsoft a Google. Poté se pro potřeby porovnání stanovila čtyři kritéria zaměřená na bezpečnost. U každého kritéria zvlášť pak bylo provedeno vzájemné porovnání poskytovatelů. Tato porovnání pak posloužila jako podklady, ze kterých se vycházelo při tvorbě pořadí variant ve vícekriteriální analýze variant. Vznikl také souhrnný přehled o bezpečnostních aspektech jednotlivých poskytovatelů. Dále následovalo samotné provedení vícekriteriální analýzy variant, kde prvním krokem bylo stanovení vah kritérií pomocí metody pořadí. Poté bylo určeno pořadí variant, jejich ohodnocení a vypočteno výsledné pořadí variant pomocí metody pořadí s váhami. Na prvním místě se umístil Google, po něm následoval Microsoft a jako třetí se umístil Amazon. Na základě této analýzy byl Google vybrán jako poskytovatel, kterého by autor doporučil pro firmy ze sektoru malých a středních podniků. Další doporučení pro firmy ze sektoru malých a středních podniků byla formulována v kapitole Doporučení.

7 Seznam použitých zdrojů

7.1 Literární zdroje

MURUGESAN, San a Irena BOJANOVA, ed. *Encyclopedia of Cloud Computing*. Chichester: Wiley, 2016. ISBN 978-1-118 82197-8.

VELTE, Anthony T.; VELTE, Toby J. a ELSENPETER, Robert. Cloud Computing: A Practical Approach. McGraw-Hill, 2010 ISBN 978-0-07-162695-8.

YANG, Chaowei a Qunying HUANG. Spatial Cloud Computing A Practical Aproach CRC Press, 2013. ISBN 978-1-4665-9317-6.

7.2 Internetové zdroje

AKTUÁLNĚ.CZ, 2011. *Cloud*. Online. In: Aktuálně.cz. Dostupné z: https://www.aktualne.cz/wiki/veda-a-technika/cloud/r~i:wiki:1998/. [cit. 2023-08-16].

ABANDY, Roosevelt, 2022. *The History of Microsoft Azure*. Online. In: Microsoft Community Hub. Dostupné z: https://techcommunity.microsoft.com/t5/educator-developer-blog/the-history-of-microsoft-azure/ba-p/3574204. [cit. 2024-03-14].

AMAZON

- AMAZON, 2019. *Aligning to the NIST CSF in the AWS Cloud*. Online. In: Amazon Web Services. Dostupné z: https://pages.awscloud.com/rs/112-TZM-766/images/NIST_Cybersecurity_Framework_CSF.pdf. [cit. 2024-03-14].
- AMAZON, 2023. *AWS DATA PROCESSING ADDENDUM*. Online. In: Amazon Web Services. Dostupné z: https://d1.awsstatic.com/legal/aws-dpa/aws-dpa.pdf. [cit. 2024-03-14].
- AMAZON, 2024. *Overview of Amazon Web Services*. Online. In: Amazon Web Services. Dostupné z: https://docs.aws.amazon.com/pdfs/whitepapers/latest/aws-overview/aws-overview.pdf?did=wp_card&trk=wp_card. [cit. 2024-03-14].
- AMAZON, c2024a. *AWS Global Infrastructure*. Online. In: Amazon Web Services. Dostupné z: https://aws.amazon.com/about-aws/global-infrastructure/?p=ngi&loc=0. [cit. 2024-03-14].

- AMAZON, c2024b. *ENVIRONMENTAL LAYER*. Online. In: Amazon Web Services. Dostupné z: https://aws.amazon.com/compliance/data-center/environmental-layer/. [cit. 2024-03-14].
- AMAZON, c2024c. *MPA & Studio Security*. Online. In: Amazon Web Services. Dostupné z: https://aws.amazon.com/compliance/mpa/. [cit. 2024-03-14].
- AMAZON, c2024d. *Our Controls*. Online. In: Amazon Web Services. Dostupné z: https://aws.amazon.com/compliance/data-center/controls/. [cit. 2024-03-14].
- AMAZON, c2024e. *PERIMETER LAYER*. Online. In: Amazon Web Services. Dostupné z: https://aws.amazon.com/compliance/data-center/perimeter-layer/. [cit. 2024-03-14].

BAIRAGI, Swati a BANG, Ankur, 2015. *Cloud Computing: History, Architecture, Security Issues*. Online. In: ResearchGate. Dostupné z: https://www.researchgate.net/publication/323967455_Cloud_Computing_History_Architecture_Security_Issues. [cit. 2023-09-28].

BUSINESSINFO.CZ, 2021. *Uplatňování definice malého a středního podniku (MSP)*. Online. In: BusinessInfo.cz. Dostupné z: https://www.businessinfo.cz/navody/uplatnovani-nove-definice-maleho-a/. [cit. 2024-02-21].

CompTIA

a. COMPTIA. *What Is SaaS?* Online. In: CompTIA. Dostupné z: https://www.comptia.org/content/articles/what-is-saas. [cit. 2023-09-01].
b. COMPTIA. *What Is PaaS?* Online. In: CompTIA. Dostupné z: https://www.comptia.org/content/articles/what-is-paas. [cit. 2023-09-01].
c. COMPTIA. *What Is IaaS?* Online. In: CompTIA. Dostupné z: https://www.comptia.org/content/articles/what-is-iaas. [cit. 2023-09-01].

FOOTE, Keith D., 2021. *A Brief History of Cloud Computing*. Online. In: DATAVERSITY. Dostupné z: https://www.dataversity.net/brief-history-cloud-computing/. [cit. 2023-08-16].

GARTNER, c2023. *Cloud Computing*. Online. In: Gartner. Dostupné z: https://www.gartner.com/en/information-technology/glossary/cloud-computing. [cit. 2023-09-27].

GILLIS, Alexander S., 2020. *Thick client (fat client)*. Online. In: TechTarget. Dostupné z: https://www.techtarget.com/whatis/definition/fat-client-thick-client. [cit. 2023-10-18].

GILLIS, Alexander S., 2021. *Thin client (lean client)*. Online. In: TechTarget. Dostupné z: https://www.techtarget.com/searchnetworking/definition/thin-client. [cit. 2023-10-18].

GOOGLE

- GOOGLE, 2022a. *Data incident response process*. Online. In: Google Cloud. Dostupné z: https://cloud.google.com/docs/security/incident-response. [cit. 2024-03-14].
- GOOGLE, 2022b. *Default encryption at rest*. Online. In: Google Cloud. Dostupné z: https://cloud.google.com/docs/security/encryption/default-encryption#googles_default_encryption. [cit. 2024-03-14].
- GOOGLE, 2023a. *Expanding our infrastructure around the world*. Online. In: Google Cloud. Dostupné z: https://cloud.google.com/blog/products/infrastructure/expanding-cloud-infrastructure-around-the-world. [cit. 2024-03-14].
- GOOGLE, 2023b. *Google security overview*. Online. In: Google Cloud. Dostupné z: https://cloud.google.com/docs/security/overview/whitepaper#operational_security. [cit. 2024-03-14].
- GOOGLE, 2024. *Data encryption options*. Online. In: Google Cloud. Dostupné z: https://cloud.google.com/storage/docs/encryption. [cit. 2024-03-14].

GOOGLE CLOUD TECH, 2020. *Google Data Center Security: 6 Layers Deep*. Online. In: YouTube. Dostupné z: https://www.youtube.com/watch?v=kd33UVZhnAA. [cit. 2024-03-14].

KASPERSKY, c2023. *What is Cloud Security?* Online. In: Kaspersky. Dostupné z: https://usa.kaspersky.com/resource-center/definitions/what-is-cloud-security. [cit. 2023-11-17].

KUMAR, Atul, 2023. *Cloud Deployment Models: Everything about Public, Private and Hybrid*. Online. In: K21Academy. Dostupné z: https://k21academy.com/cloud-blogs/cloud-computing-deployment-models/. [cit. 2023-08-26].

MELL, Peter a GRANCE, Timothy, 2011. The NIST Definition of Cloud Computing. Online. In: *Special Publication 800-145*. Dostupné z: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf. [cit. 2023-08-17].

MICROSOFT

- MICROSOFT, 2023a. *Azure facilities, premises, and physical security*. Online. In: Microsoft Learn. Dostupné z: https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security. [cit. 2024-03-14].
- MICROSOFT, 2023b. *Azure infrastructure availability*. Online. In: Microsoft Learn. Dostupné z: https://learn.microsoft.com/en-us/azure/security/fundamentals/infrastructure-availability. [cit. 2024-03-14].
- MICROSOFT, 2023c. *Microsoft Support and Professional Services and Breach Notification Under the GDPR*. Online. In: Microsoft Learn. Dostupné z: https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-microsoft-support-professional-services. [cit. 2024-03-14].
- MICROSOFT, c2023. *Co jsou veřejné, privátní a hybridní cloudy?* Online. In: Microsoft Azure. Dostupné z: https://azure.microsoft.com/cs-cz/resources/cloud-computing-dictionary/what-are-private-public-hybrid-clouds. [cit. 2023-08-26].
- MICROSOFT, 2024a. *Data encryption models*. Online. In: Microsoft Learn. Dostupné z: https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-models. [cit. 2024-03-14].
- MICROSOFT, 2024b. *Microsoft Azure, Dynamics 365, and Power Platform breach notification under the GDPR*. Online. In: Microsoft Learn. Dostupné z: https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-azure-dynamics. [cit. 2024-03-14].
- MICROSOFT, c2024. *Globální infrastruktura Azure*. Online. In: Microsoft Azure. Dostupné z: https://azure.microsoft.com/cs-cz/explore/global-infrastructure/. [cit. 2024-03-14].

PERRY, Yifat, 2022. *AWS KMS Encryption: Server-Side Encryption for Data in AWS*. Online. In: NetApp BlueXP. Dostupné z: https://bluexp.netapp.com/blog/aws-cvo-blg-aws-kms-encryption-server-side-encryption-for-data-in-aws. [cit. 2024-03-14].

PWC, 2019. *Bezpečnost cloudových služeb*. Online. In: Pwc. Dostupné z: https://www.pwc.com/cz/cs/cyberandprivacy/bezpecnost%20cloudovych%20sluzeb.pdf. [cit. 2024-03-14].

SHAMEEM, P. Mohamed a SHAJI, R.S., 2013. *Components make up of Cloud Computing Solution*. Online. In: ResearchGate. Dostupné z: https://www.researchgate.net/publication/289259494/figure/fig1/AS:392626940465155@1470620965949/Components-make-up-of-Cloud-Computing-Solution.png. [cit. 2023-10-13].

STOUFFER, Clare, 2023. *23 cloud security risks, threats, and best practices to follow*. Online. In: Norton. Dostupné z: https://us.norton.com/blog/privacy/cloud-security-risks. [cit. 2023-11-17].

SYNERGY RESEARCH GROUP, 2023. *AI Helps to Stabilize Quarterly Cloud Market Growth Rate; Microsoft Market Share Nudges Up Again*. Online. In: Synergy Research Group. Dostupné z: https://www.srgresearch.com/articles/ai-helps-to-stabilize-quarterly-cloud-market-growth-rate-microsoft-market-share-nudges-up-again. [cit. 2024-03-14].

THREAT INTEL, 2018. *A Brief History of Cloud Computing*. Online. In: Medium. Dostupné z: https://medium.com/threat-intel/cloud-computing-e5e746b282f5. [cit. 2023-08-16].

8 Seznam obrázků, tabulek, grafů a zkratek

8.1 Seznam obrázků

Obrázek 1 Řešení cloud computingu 3 základními komponenty 23

8.2 Seznam tabulek

Tabulka 1 Přehled o šifrování v klidu – Amazon 43
Tabulka 2 Přehled o šifrování v klidu – Microsoft 44
Tabulka 3 Přehled o šifrování v klidu – Google 45
Tabulka 4 Porovnání poskytovatelů.....45
Tabulka 5 Porovnání poskytovatelů.....49
Tabulka 6 Stanovení vah metodou pořadí.....50
Tabulka 7 Pořadí variant 51
Tabulka 8 Seřazení variant.....51

8.3 Seznam grafů

Graf 1 Počet standardů, certifikací či právních předpisů 36

8.4 Seznam použitých zkratek

ARPANET	Advanced Research Projects Agency NETwork
NIST	National Institute of Standards and Technology
SaaS	Software as a Service
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
DSaaS	Data storage as a Service
AaaS	Analytics as a Service
DaaS	Desktop as a Service
SecaaS	Security as a Service
IAMaaS	Identity and Access Management as Service
MaaS	Monitoring as a Service
PDA	Personal Digital Assistant

IAM	Identity and Access Management
VPN	Virtual private network
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
IP	Internet Protocol
API	Application Programming Interface
DoS	Denial of Service
DDoS	Distributed Denial of Service
IT	Information technology
EUR	Společná evropská měnová jednotka
AWS	Amazon Web Services
IoT	Internet of Things
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
CSA STAR	Cloud Security Alliance The Security, Trust, Assurance, and Risk
SOC	System and Organization Controls
CoC	EU Cloud Code of Conduct
C5	Cloud Computing Compliance Controls Catalogue
PCI DSS	Payment Card Industry Data Security Standard
S3	Simple Storage Service
SSE	Server-side encryption
AES	Advanced Encryption Standard
KMS	Key Management Service
COE	Correction of Error document
SSE-C	SSE with customer provided encryption keys
SSE-S3	SSE with Amazon S3 managed encryption keys
SSE-KMS	SSE with AWS KMS stored encryption keys