Cloud computing

Cloud computing je novou výpočtovou paradigmou a ako taký vyvolal mnohé zmeny v oblastiach IT vrátane ukladania údajov, počítačovej architektúry, sietí, správy zdrojov, plánovania a v neposlednom rade počítačovej bezpečnosti.

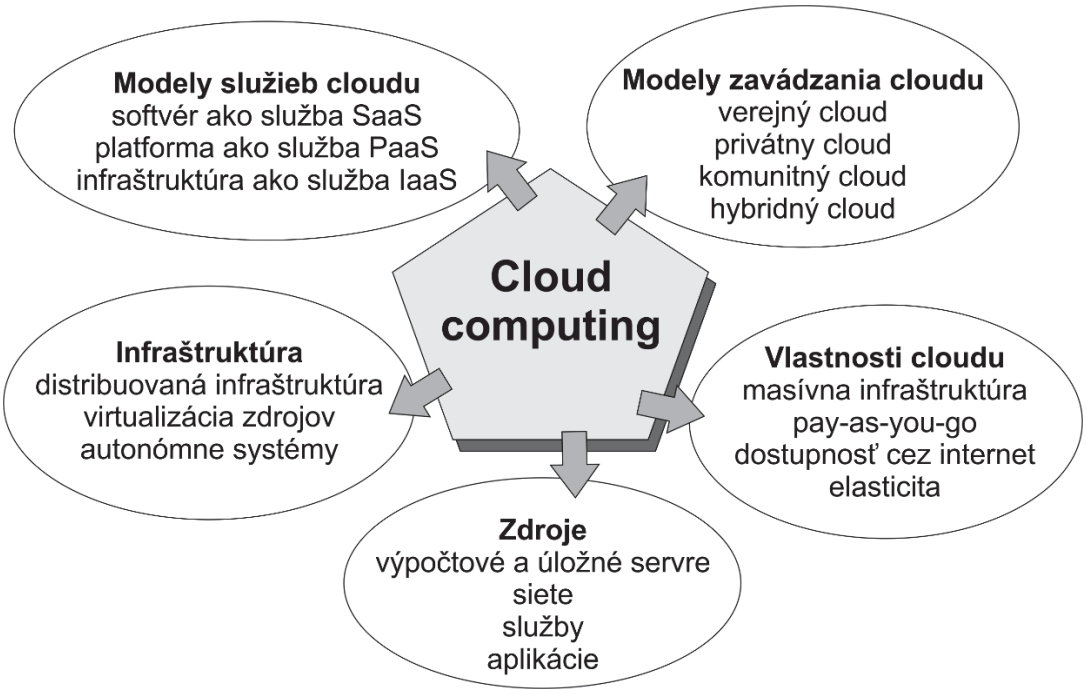
V roku 2011 NIST (Národný inštitút pre normy a technológie USA) definoval cloud computing ako „model umožňujúci všadeprítomný, pohodlný sieťový prístup na požiadanie k zdieľanému zoskupeniu konfigurovateľných výpočtových zdrojov (napr. sietí, serverov, úložísk, aplikácií a služieb), ktoré možno rýchlo poskytnúť a uvoľniť s minimálnym úsilím v oblasti riadenia alebo interakcie poskytovateľov služieb.“ [MG11]

Medzinárodná organizácia pre normalizáciu (ISO) poskytuje obdobnú definíciu, kde je cloud computing definovaný ako „vyvíjajúca sa paradigma“: „Cloud computing je paradigma umožňujúca sieťový prístup k škálovateľnému a elastickému zoskupeniu zdieľateľných fyzických alebo virtuálnych zdrojov so samoobslužným prístupom a správou na požiadanie“ [ISO14]. Spoločnosť Gartner definuje cloud computing zjednodušene ako „Štýl výpočtu, pri ktorom sú škálovateľné a elastické IT schopnosti poskytované ako služba viacerým zákazníkom využívajúcim internetové technológie“ [G19].

Cloud computing sa vyznačuje piatimi kľúčovými vlastnosťami: 1. prístup cez sieť/Internet, 2. cloud je samoobslužný na požiadanie, 3. združovanie zdrojov alebo zdieľané služby, 4. vysoká elasticita (pružnosť) a 5. merateľnosť služby [R16].

Cloud má tri základné modely poskytovania cloudových služieb: SaaS – softvér ako služba, PaaS – platforma ako služba a IaaS – infraštruktúra ako služba. Medzi štyri základné modely nasadenia cloudu patrí: súkromný cloud, komunitný cloud, verejný cloud a hybridný cloud [M17]. Uvedeným modelom je venovaný väčší priestor v ďalších častiach učebnice.

Cloud computing poskytuje používateľom prostriedky na jednoduché využitie výpočtových zariadení kedykoľvek a odkiaľkoľvek. Používatelia sa nemusia starať o vybudovanie vlastnej infraštruktúry, nákup nového vybavenia alebo investície do obstarávania licencovaného softvéru. Okrem toho majú používatelia cloudu za určitý finančný obnos prístup k potrebnému, či už veľkému alebo malému, výpočtovému výkonu, alebo dátovému úložisku.



Obrázok 0-1 Cloud computing: modely služieb, modely zavádzania, vlastnosti, zdroje a organizácia infraštruktúry.

Cloud a cloud computing je nový model výpočtovej techniky, ktorý je integráciou pokročilých výpočtových modelov, sofistikovaných webových technológií a moderných technológií sieťovej komunikácie (najmä vysokorýchlostného Internetu).

Zo zavedenia cloud computingu môžu ťažiť viaceré oblasti spoločnosti, ako sú napríklad vedecké a technické inštitúcie, dolovanie dát, hry a sociálne siete, ako aj mnohé ďalšie výpočtové a dátovo náročné činností. V cloude je možné uložiť širokú škálu údajov od výsledkov fyzikálnych experimentov, cez finančné údaje alebo údaje o podnikovom riadení, až po osobné údaje, ako sú fotografie, videá a filmy. Veľkou výhodou je dostupnosť informácií z akéhokoľvek miesta, kde je možné pripojiť sa k internetu. Navyše, informácie uložené v cloude sa dajú ľahko zdieľať. Uvedená skutočnosť však otvára aj mnohé obavy vzhľadom na bezpečnosť a súkromie údajov.

Výpočtové cloudy sú výkonnými pomocníkmi a aktivátormi zmien v organizáciách. Cloud computing výrazne zmenil a zmení spôsob, akým ľudia a organizácie používajú počítače a ich pracovné postupy, ako aj spôsob, akým spoločnosti a vlády zavádzajú svoje počítačové aplikácie. Napríklad v roku 2019 americká armáda vyhlásila víťaza tendra za 10mld dolárov na cloudové služby, ktorým sa stala spoločnosť Microsoft so svojim cloudom Azure. Armáda si objednala cloudové služby v takom veľkom rozsahu, pretože interne nedokáže dodávať jednotkám dáta v kvalite a rýchlosti, akú potrebujú.

Aj uvedený fakt nasvedčuje, že cloud má potenciál výrazne zlepšiť prístup k informáciám pre všetkých, ako aj znížiť náklady na IT. Prebiehajúci vývin cloudov, zavádzanie nových platforiem a aplikácií pre cloud computing, rast v zavádzaní služieb cloud computingu a vznik otvorených štandardov pre cloud computing zvýšil a naďalej

bude zvyšovať príťažlivosť tejto technológie pre používateľov, ale aj pre samotných poskytovateľov cloudových služieb.

Ako vyplýva z vyššie uvedených definícii cloudu, jednou z vlastností cloudu je škálovateľnosť. *Škálovateľnosť* je schopnosť systému zachovávať rovnaký výkon, aj keď sa veľkosť systému zvyšuje alebo znižuje. Je to schopnosť pracovať s náhlymi zmenami potreby obsluhy čiže zvyšovať sledované parametre v prípade, že takáto potreba nastane. V užšom zmysle je to nielen schopnosť vydržať náhlu záťaž, ale tiež hospodárnosť, ak vysoký výkon momentálne nie je potreba. Napríklad, webový server, ktorý zvyčajne prijíma 500 žiadostí za minútu a reaguje s dobou odozvy 15 ms, by po náraste žiadostí na 1000 za minútu nemal reagovať s prístupovým časom až 500 ms. Toto nie je očakávané správanie systému a ani škálovateľnosť, pretože sa neočakáva až taký dramatický dopad na dobu odozvy. Pri škálovateľnom systéme sa očakáva, že jeho výkon bude ovplyvnený úmerne so zmenou veľkosti alebo požiadaviek, a preto odozva servera mala byť len o pár milisekúnd väčšia (napr. dvakrát väčšia). Zníženie výkonu spôsobené zvýšeným pracovným zaťažením je možné vykompenzovať napríklad pridaním hardvéru [FH17].

Modely služieb cloudu

Výpočtový alebo sieťový prostriedok, aplikácia alebo akýkoľvek iný druh IT služby ponúkanej používateľovi prostredníctvom cloudu sa nazýva *cloudová služba*. Cloudové služby siahajú od jednoduchých aplikácií, ako sú e-mail, kalendár, spracovanie textov a zdieľanie fotografií, až po rôzne typy komplexných podnikových aplikácií a výpočtové zdroje ponúkané ako služby hlavnými poskytovateľmi.

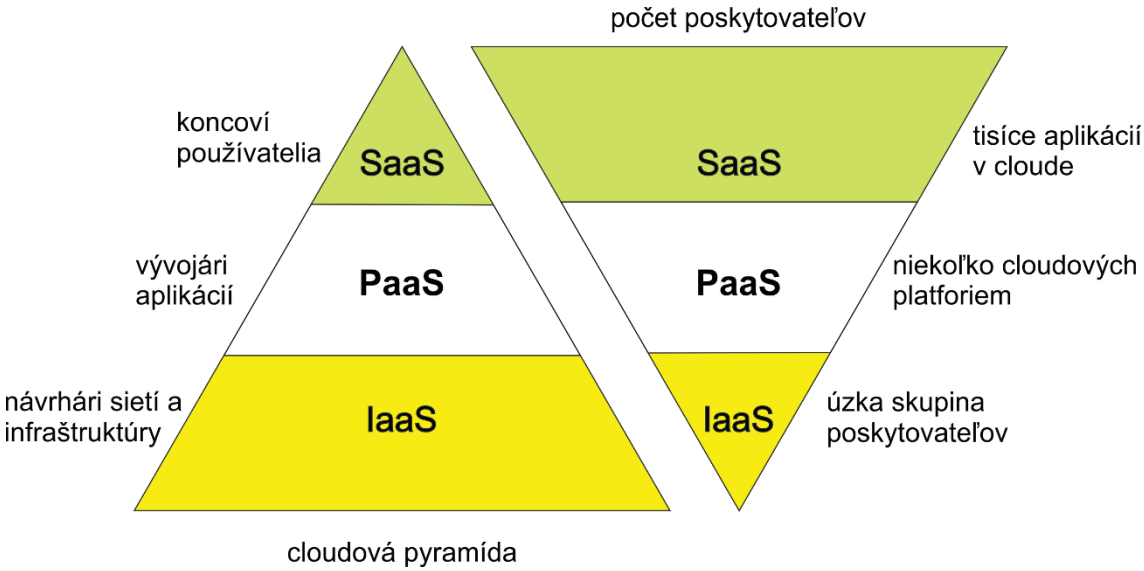
Cloud computing sa vyvinul z tradičného modelu outsourcingu. V modeli outsourcingu poskytuje potrebnú službu organizácia, ktorá sa špecializuje na špecifickú oblasť. Zmluvná organizácia si vyberie konkrétne obdobie, na ktoré jej bude služba poskytnutá. Iný spôsob tradičného modelu je, keď podnik namiesto outsourcingu svojich informačných systémov uzavrie zmluvu s externými odborníkmi na správu svojich interných informačných systémov. V oboch prípadoch bol informačný systém pod kontrolou tretej strany. Tretia strana často spracovala aj všetky súvisiace údaje. V tradičnom modeli nemali podniky problém s uzavretou dohodou, sporné body si ošetrili podrobnými ustanoveniami v zmluve s treťou stranou.

Z toho vychádza aj model cloud computingu. Hlavnou atraktívnosťou cloud computingu pre podniky je jeho schopnosť poskytnúť podniku plne funkčný počítačový systém do niekoľkých hodín alebo niekoľkých dní, v závislosti od úrovne zložitosti vo vybranom systéme. Platforma cloud computing poskytuje zákazníkom všetky možnosti, ako napríklad typ potrebného hardvéru, typ služby, potrebné aplikácie, množstvo úložného priestoru, atď., aby si mohli vybrať a spustiť svoj systém. Navyše, služba je k dispozícii bez potreby údržby a samotného riadenia služby, čo by si inak od organizácie vyžadovalo značné finančné aj ľudské zdroje.

V závislosti od typu ponúkaných služieb možno cloudové služby rozdeliť do troch hlavných kategórií: *softvér ako služba* (SaaS), *platforma ako služba* (PaaS) a

infraštruktúra ako služba (IaaS). Okrem týchto základných služieb je v ponuke niekoľko ďalších služieb podpory cloudu, napríklad bezpečnosť ako služba a správa identity a prístupu ako služba. Každá kategória služieb sa môže používať samostatne alebo v kombinácii s ostatnými. Zákazníci si môžu vybrať rôznych poskytovateľov cloudových služieb. Na trhu sú vďaka konkurencii dostupné rôzne cenové ponuky cloudových služieb. V prostredí cloud computingu sa softvér, ktorý beží na pozadí na účely podpory integrácie a monitorovania, nazýva *middleware* [B17, M17].

Nižšie uvedený Obrázok 0-2 uvádza zovšeobecnený pohľad na tri základné modely služieb cloudu, ich nadväznosť, ako aj ich úroveň nasadenia na trhu spolu s ich komplexnosťou.



Obrázok 0-2 Porovnanie základných modelov služieb v cloude.

Softvér ako služba (SaaS)

V modeli *softvér ako služba* (SaaS, Software as a Service) je aplikácia spravovaná poskytovateľom cloudu a dodáva sa ako služba používateľom, predovšetkým prostredníctvom internetu alebo vyhradenej siete. Eliminuje potrebu inštalovať a spúšťať aplikáciu lokálne na počítači používateľa, a tým tiež zbavuje používateľov bremena údržby hardvéru a softvéru a inovácií. Softvérová licencia nie je vlastníctvom používateľa. Náklady na používanie služby sa však stávajú pre organizáciu skôr stálou záťažou ako jednorazovým počiatočným kapitálovým nákladom v čase nákupu.

SaaS poskytuje hardvér a softvér servera organizácii bez toho, aby organizácia mala akékoľvek starosti pri správe IT systému. Najjednoduchším príkladom služby SaaS pre organizáciu je poskytovanie e-mailu. Na druhej strane, aj poskytovateľ cloudu má výhody a finančné úspory pri prevádzkovaní služby vyplývajúce z rozsahu spravovania veľkej infraštruktúry a jeho silnej pozície v danej oblasti. Je schopný poskytnúť potrebné výpočtové zdroje za dostupnú cenu používateľom, z ktorých väčšinu tvoria malé a stredné podniky. SaaS ponecháva úplnú kontrolu nad výpočtovým systémom poskytovateľom.

Organizácia si vyberá len softvér, ktorý potrebuje, z kolekcie softvéru ponúkaného poskytovateľom cloudových služieb.

Ak by organizácia mala softvér zakúpený lokálne, spravovanie softvéru, napríklad balíka kancelárskych aplikácií, si vyžaduje pre organizáciu činnosti, čas a financie navyše, ako napr. udržiavanie aktuálnej verzie, potrebné licencie pre všetkých používateľov, správu opráv a aktualizáciu softvéru. Napríklad malý podnik zameraný na výrobu automobilovej súčiastky musí udržiavať svoju výrobnú kvalitu, presúvať výrobky v dodávateľskom reťazci k výrobcovi automobilov a udržiavať alebo rozvíjať svoje podnikanie. Pre takýto podnik by správa IT systému znamenala zbytočnú záťaž navyše. Využitie modelu SaaS je ideálne riešenie jeho situácie. V súčasnosti s nárastom technológie umožňuje model SaaS používateľovi integrovať naraz výsledky viacerých aplikácií. V tradičnom modeli predajcovia predávali softvérové aplikácie používateľom za jednorazový poplatok a používatelia boli zodpovední za udržiavanie softvérových aktualizácií, ktoré predajca poskytoval. V modeli SaaS však predajca, alebo tretia strana známa ako agregátor, poskytujú softvérovú aplikáciu cez cloud. Používateľ platí priebežný poplatok za používanie softvéru a nemusí sa starať o jeho údržbu [S14].

Ľahká implementácia SaaS má tiež potenciálne nevýhody. Rôzne oddelenia v rámci firmy objavia špecializované aplikácie, ktoré považujú za potrebné pre svoju efektívnejšiu činnosť, následne ich nájdu aj v cloude a v modeli SaaS ich vedia aj rýchlo nasadiť. Uvedený prístup by však mohol viesť k hromadeniu aplikácií, ktoré podnik používa, a organizácia môže mať ťažkosti s integráciou výstupov z množstva rôznych aplikácií, rovnako ako aj s navyšovaním ceny za využité služby. Preto by podniky mali mať pri používaní SaaS strategickú víziu a kontrolné mechanizmy.

Ako príklad modelu SaaS je možné zobrať produkt Microsoft Office 365. Ide o cloudovú službu poskytovanú spoločnosťou Microsoft, ktorá sprístupňuje všetky svoje popredné softvérové produkty pre kancelárske činnosti. Služba Office 365 nielenže prichádza so softvérom, ktorý sú ľudia zvyknutí používať na svojich vlastných počítačoch, ale poskytuje aj úložisko pre dokumenty vytvorené pomocou tejto služby. Uvedená funkcia umožňuje používateľovi prístup k svojim dokumentom odkiaľkoľvek a z viacerých zariadení. Navyše, mobilita zamestnancov je v dnešnej dobe vysoká, preto je nevyhnutné mať možnosť pristupovať k dokumentom na viacerých zariadeniach, bez ohľadu na to, aké rôzne operačné systémy používajú. Namiesto toho, aby sa podnik snažil spravovať softvér na všetkých zariadeniach, ktoré ich zamestnanci používajú v rôznych lokalitách, zaplatením si služby Office 365, získava potrebné zdieľanie dokumentov a ich správy ako cloudovú službu. Podobnú službu poskytuje aj Google Apps, ktorý poskytuje podobné nástroje prostredníctvom cloudu bezplatne [B17, S14].

Medzi ďalšie príklady služieb SaaS patrí Webmail, Google Apps, Microsoft Office 365, SAP, IBM Cloud, Oracle Applications.

Platforma ako služba (PaaS)

V modeli *platforma ako služba* (PaaS, Platform as a Service) sú platforma a nástroje na vývoj aplikácií a middlewarové systémy hosťované poskytovateľom cloudu. Model PaaS umožňuje vývojárom jednoducho programovať vyvíjané aplikácie a implementovať ich bez priamej interakcie s podkladovou infraštruktúrou. Model PaaS ponúka množstvo nástrojov a zariadení potrebných na vytváranie a poskytovanie aplikácií, ako aj služby na návrh aplikácií, vývoj, testovanie, nasadenie a hosting, a aj aplikačné služby, ako je integrácia webových služieb, integrácia databáz, bezpečnosť, ukladanie, tímová komunikácia a spolupráca.

Na rozdiel od modelu SaaS, organizácia používajúca PaaS musí mať náležitých počítačových špecialistov na správu platformy, ktorú si predplatila. PaaS prináša flexibilitu cloudovej platformy aj z pohľadu dostupnosti zdrojov, aj z pohľadu pružnosti dopytu. Príkladom platformy, ktorú PaaS poskytuje zákazníkovi, môže byť operačný systém MS Windows, s potrebnou kapacitou servera na spustenie potrebných aplikácií. Poskytovateľ cloudových služieb PaaS spravuje systém pre jeho údržbu a poskytovanie nástrojov, ako sú .NET a Java, zatiaľ čo zákazník je zodpovedný iba za výber aplikácií, ktoré bežia na platforme podľa svojho výberu pomocou dostupných nástrojov. Zákazník je tak zodpovedný za bezpečnosť spojenú s aplikáciami, ktoré spúšťa. Napríklad, zákazník prevádzkujúci databázu Microsoft SQL Server na zvolenej platforme by si mal byť vedomý zraniteľností databázového systému. Zákazník by preto mal mať odborné znalosti na riadenie takýchto aplikácií nad použitou platformou. Jednou z hlavných výhod pre zákazníka je, že ak je potrebná zmena hardvéru, alebo ak niektoré iné aplikácie vyžadujú inú platformu, ich uvedenie do prevádzky trvá oveľa kratší čas [S14].

Pretože model PaaS je k dispozícii prostredníctvom cloudu, je vysoko škálovateľný. Aj keď PaaS dáva používateľovi voľnosť pri výbere aplikácií, ktoré bežia na jeho platforme, hardvérový aspekt je stále spravovaný poskytovateľom cloudu. Pre používateľa to znamená výhodu, keďže môže očakávať nepretržitú službu bez plánovaných prestojov na údržbu, ako by tomu bolo v lokálnom dátovom centre. PaaS je vhodný pre veľké spoločnosti, ktoré chcú používať PaaS na vývoj, testovanie a zavádzanie nových aplikácií založených na rôznych platformách. Pretože náklady na infraštruktúru využívajú model priebežného financovania, mnohé firmy sú schopné používať rôzne platformy pre svoje aplikácie. Navyše, vzhľadom na ľahké použitie pre koncového používateľa je možné aplikácie testovať interaktívnym spôsobom pre viacerých súbežných používateľov. Ďalšou výhodou modelu PaaS je, že vývojárom umožňuje vytvárať distribuované tímy, ktoré pracujú súčasne na rôznych častiach svojej aplikácie, a priradiť rôznym používateľom rôzne úrovne prístupu a sledovať ich vzorce používania počas testovacej fázy. PaaS tak ponúka flexibilnú architektúru nájomcov.

Okrem toho, PaaS podporuje celý životný cyklus vývoja aplikácií. Tento proces zahŕňa poskytnutie takých funkcií, ktoré zákazník môže kombinovať spôsobom akým potrebuje a vytvoriť tak žiadané aplikácie. Vývojári aplikácií nemusia byť tradičnými programátormi, ale skôr používateľmi v praktickom prostredí. Funkcie PaaS podporujú

schopnosť zhromažďovať logovacie súbory používateľského správania a identifikovať možné problémy, ktoré vznikli, keď reálny používateľ vyskúšal aplikáciu. Je vhodné, aby platforma podporovala Application Lifecycle Management (ALM, Správa životného cyklu aplikácií), nakoľko je potom ľahké implementovať budúce zmeny [B17, S14].

Potenciálny používateľ pred rozhodnutím o konkrétnom poskytovateľovi PaaS by mal vyhodnotiť nasledovné aspekty [S14]:

- Podporuje platforma viac-nájom v architektúre a aplikáciách, t. j. architektúru, v ktorej jedna inštancia softvérovej aplikácie slúži viacerým zákazníkom?
- Ktoré aplikácie správy životného cyklu aplikácií sú podporované?
- Aké aplikačné programovacie rozhrania (API) sú podporované?
- Uľahčuje platforma škálovateľnosť?
- Aké typy údajov logovacích súborov sú dostupné pre používateľa?
- Ktoré programovacie jazyky platforma podporuje?

Medzi príklady modelu PaaS patrí Google App Engine, Microsoft Azure, Amazon web services, SAP a Sun Microsystems NetBeans IDE, ale aj open source ako Cloud Foundry a OpenShift.

Infraštruktúra ako služba (IaaS)

V cloudovom modeli *infraštruktúra ako služba* (IaaS, Infrastructure as a Service) sa ako služba dodáva základná počítačová infraštruktúra ako sú servery, CPU, úložisko, sieťové zariadenia a zariadenia dátových centier. Namiesto nákupu týchto zdrojov ich zákazník získa ako outsourcované služby na obdobie, počas ktorého ich potrebuje.

IaaS poskytuje zákazníkovi rovnaké vlastnosti ako PaaS, ale zákazník je plne zodpovedný za kontrolu prenajatej infraštruktúry. Na IaaS sa dá pozerať ako na počítačový systém zákazníka, ktorý ale nevlastní. Organizácia, ktorá potrebuje výpočtové zdroje, do nich takto priamo neinvestuje, ale získava požadované zdroje prenájmom na určitú dobu. Na rozdiel od systému PaaS vyžaduje model IaaS, aby organizácia mala potrebných ľudí s rozsiahlymi skúsenosťami s výpočtovou technikou. Zákazník IaaS je zodpovedný za všetky aspekty zabezpečenia systému, ktoré používa, s výnimkou fyzickej bezpečnosti (kontrola vstupu pred neautorizovanými osobami, bezpečnosť podpornej infraštruktúry), ktoré rieši poskytovateľ cloudu.

Typické použitie pre model IaaS je napríklad tvorba softvérovej aplikácie, kde softvéroví vývojári využívajú virtuálne počítače poskytovateľa cloudových služieb. Aplikáciu potrebujú prispôsobovať potrebám rôznych zákazníkov jej spúšťaním na viacerých virtuálnych serveroch. V takomto prípade sú najmä veľké organizácie z danej oblasti schopné naplno využiť dostupnosť virtuálnych strojov v infraštruktúre, ako aj virtuálne stroje spravovať na prevádzkovanie svojich špecializovaných aplikácií. Zo základných troch modelov služieb cloudu je IaaS najdrahší model a využívajú ho predovšetkým veľké spoločnosti. Použitie IaaS je často iba doplnkom k interným výpočtovým zdrojom organizácie, keď organizácia potrebuje nárazovo, dočasne rozšíriť

svoju infraštruktúru. Ako je opísané vyššie, IaaS je možné nasadiť aj pre aplikácie využívajúce prostredie virtuálnych strojov [S14].

Silnou stránkou IaaS modelu služieb cloudu je, že jednoducho dáva možnosť veľkým organizáciám zvýšiť si svoje IT zdroje. Vďaka IaaS sú organizácie schopné modernizovať svoju IT infraštruktúru bez toho, aby investovali kapitálové výdavky do podnikovej IT infraštruktúry. Keďže organizácie platia iba za cloudové prostriedky, ktoré používajú, model IaaS ponúka obvyklé výhody cloudu a zároveň dáva zákazníkovi väčšiu kontrolu nad bezpečnostnými aspektmi aplikácií, ktoré bežia vo virtualizovanom prostredí. Rozsah použitia modelu IaaS je široký. Organizácie môžu IaaS využívať ako výpočtový výkon, či už hardvérový, alebo softvérový. Môžu IaaS použiť aj na konkrétne účely, napríklad na ukladanie dát, zabezpečenie alebo vytváranie sietí.

Pretože organizácia priamo kontroluje na čo sa infraštruktúra používa, má nielen prístup k výpočtovým zdrojom, ale aj kontrolu nad infraštruktúrou. Hlavným dôvodom, prečo sa snaží organizácia získať dodatočný výpočtový výkon, je snaha nájsť spôsob ako vzájomne prepojiť viaceré aplikácie. Aplikácie nemusia byť ani IaaS. Môže ísť o aplikácie PaaS alebo SaaS. Organizácia potrebuje dostatočne veľa testovať rôzne scenáre vzájomného prepojenia a k tomu potrebuje ďalší hardvér. Navyše hardvér bez obmedzení a bez firemných bezpečnostných politík, ktorý by mohol zakazovať napríklad presun údajov medzi platformami. IaaS poskytuje potrebnú infraštruktúru pod kontrolou organizácie, ale bez obmedzení. Podobne môže mať organizácia potrebu dočasne ukladať veľké objemy dát počas nejakého obdobia. V tomto prípade sa organizácia musí pozrieť na povahu úložiska, t. j. či je zdieľané v prostredí viacerých nájomcov alebo je vyhradené len pre jedného používateľa. Druhý typ úložiska je drahší, ale poskytuje organizácii vyšší stupeň bezpečnosti. Nevýhodou pri ukladaní pomocou modelu IaaS je, že organizácia sa stáva zodpovednou za zálohovanie a obnovu akýchkoľvek uložených údajov, čiže nevyužíva úložisko, kde sa o zálohovanie a obnovu stará poskytovateľ cloudových služieb, ale musí sa o to postarať sama.

Vytváranie sietí a bezpečnosť sú ďalšie aspekty, v rámci ktorých organizácia môže používať IaaS. Práve bezpečnosť je najnáročnejšou časťou pri používaní IaaS. Bezpečnostné prístupy si zvyčajne vyžadujú úplnú kontrolu nad infraštruktúrou. Pri používaní modelu IaaS z pohľadu bezpečnosti sa musí organizácia vzdať fyzickej bezpečnosti infraštruktúry v prospech poskytovateľa cloudových služieb. Preto je potrebné vyberať si dôveryhodného poskytovateľa. Následne organizácia musí byť schopná nasadiť svojich zamestnancov, ktorí sa budú vytvárať potrebné politíky zabezpečenia prístupu, ako aj ich implementáciu. Z pohľadu sietí, prínos modelu IaaS spočíva v schopnosti nasadiť rôzny hardvér z viacerých lokalít na prepojenie rôznych segmentov organizácie rozmiestnených v rôznych geografických oblastiach. Pretože služba je modelom pay-as-you-go, IaaS uľahčuje nasadenie potrebnej infraštruktúry [B17, S14].

Model IaaS má nasledujúce vlastnosti [MB16]:

- dostupnosť veľkého množstva výpočtových zdrojov, ako sú servery, sieťové vybavenie, pamäť, CPU, diskový priestor a zariadenia dátových centier na požiadanie,
- využívanie rozsiahlej infraštruktúry so zníženými nákladmi (platba za používanie), ktorá umožňuje malým a stredným podnikom využívať výhody zo združených výpočtových zdrojov,
- nástroj na zníženie tlaku na infraštruktúru zákazníckej organizácie,
- dynamická škálovateľnosť infraštruktúry, kapacita na požiadanie sa dá ľahko zväčšiť a znížiť na základe požiadaviek na zdroje.

Amazon Elastic Compute Cloud (EC2), Microsoft Azure, GoGrid, HP Enterprise Converged Infrastructure, Google Compute Engine, Cisco Cloud Infrastructure Solutions, či IBM SmartCloud Enterprise sú niektoré z príkladov modelu IaaS.

Podporné modely, Databáza ako služba DBaaS

Aby používatelia cloudov vedeli naplno a úspešne cloudy využívať, musia používať jeden alebo viac z troch základných modelov cloudových služieb – softvér ako služba (SaaS), platforma ako služba (PaaS) a infraštruktúra ako služba (IaaS). Spoločnosti využívajúce cloud sa musia však zaoberať aj niekoľkými ďalšími súvisiacimi faktormi, ako sú bezpečnosť, súkromie, správa prístupu používateľov, požiadavkami na dodržiavanie rôznych podmienok, či obnovu prevádzky. Okrem toho by zákazníci mohli potrebovať služby od viac ako jedného poskytovateľa služieb, prepájať tieto služby a integrovať ich navzájom medzi sebou a to aj so staršími aplikáciami/systémami spoločnosti. Na uľahčenie prechodu na cloud sa objavuje tzv. *cloudový ekosystém*, ktorého cieľom je ponúkať spektrum nových služieb cloudovej podpory, ktoré rozširujú, dopĺňajú alebo pomáhajú základným ponukám SaaS, PaaS a IaaS. Príkladmi takýchto služieb podpory cloudu sú ukladanie údajov ako služba (DSaaS, Data storage as a Service), analýza ako služba (AaaS, Analytics as a Service), desktop ako služba (DAAS, Desktop as a Service), bezpečnosť ako služba (SECaaS, Security as a Service), správa totožnosti a správa prístupu ako služba (IAMaaS, Identity and Access Management as a Service), a monitoring ako služba (MaaS, Monitoring as a Service), Artificial Intelligence as a Service (AIaaS) a iné [MB16].

Jedným z príkladov takéhoto modelu podpory je *databáza ako služba*. Databáza ako služba (DBaaS, Database as a Service) je cloudová služba, kde je databáza prevádzkovaná na fyzickej infraštruktúre poskytovateľa služieb. V porovnaní s lokálnou fyzickou architektúrou servera a úložiska ponúka služba cloudovej databázy nemalé výhody: okamžitú škálovateľnosť, záruku výkonnosti služby, najnovšie technológie, podporu pri zlyhaní.

Cloudový model DBaaS používa vrstvenú architektúru. Vrstva používateľského rozhrania podporuje prístup k službe cez internet. Aplikačná vrstva sa používa na prístup

k softvérovým službám a úložnému priestoru. Databázová vrstva poskytuje efektívnu a spoľahlivú databázovú službu, šetrí čas na dopytovanie a načítanie údajov opätovným použitím príkazov dotazu, ktoré sa nachádzajú v úložisku. Vrstva na ukladanie údajov údaje šifruje v momente keď sa ukladajú a to aj bez zásahu používateľa. Táto vrstva poskytuje aj správu zálohy a monitorovanie disku [MB16].

Zodpovednosť v modeloch služieb cloudu

Jednou z nosných otázok, na ktoré si používateľ cloudu musí odpovedať, je otázka za ktoré stránky bezpečnosti je pri využívaní služieb cloudu priamo zodpovedný. Otázka zodpovednosti býva pri lokálnych prostrediach väčšinou zjavná. Napríklad, organizácia vyvíjajúca softvér je zodpovedná za chyby kódu a prevádzková organizácia je zodpovedná za všetko ostatné (správnu inštaláciu softvéru, jeho správne prevádzkovanie, správne nastavenie oprávnení, atď). Snáď jednou z najväčších zmien pri prechode z lokálneho prostredia do cloudového prostredia je zložitejší model zdieľanej zodpovednosti za bezpečnosť. Hranica vymedzenia zodpovednosti poskytovateľa cloudu a používateľa cloudu sa líši v závislosti od modelu cloudovej služby.

Takmer všetci poskytovatelia cloudu sa otázkam zodpovednosti venujú vo svojej dokumentácii. Pre lepšie pochopenie rozloženia zodpovednosti medzi poskytovateľa a používateľa cloudu je použitá analógia jedenia pizze, kde je zavedená služba Pizza-as-a-Service [D19]. Existuje veľa možností ako pizzu získať. Prvou z nich je príprava pizze doma, čo si vyžaduje prístup k množstvu ingrediencií a čas na samotné vytvorenie, upečenie a zjedenie pizze. Inou možnosťou je ísť do obchodu a kúpiť si predpečenú zmrazenú pizzu, na jej prípravu je potrebná iba rúra na upečenie a miesto na zjedenie pizze. Ďalšou je možnosť zavolať si donášku pizze a zjesť ju doma. A poslednou možnosť je ísť do reštaurácie a tam si pizzu objednať aj zjesť. Diagram rôznych komponentov a kto za jednotlivé z nich zodpovedá, je uvedený na obrázku Obrázok 0-3.

Služba Pizza-as-a-Service a jej analógie sú ďalej opísané detailnejšie. Tradičný lokálny prístup je samostatná príprava pizze doma. Je potrebné si však kúpiť veľa rôznych komponentov a dať ich dohromady, byť zručný ako kuchár, no získa sa tým úplná flexibilita. Uvedené zodpovedá vytvoreniu lokálneho IT centra priamo v spoločnosti, je potrené získať hardvér, softvér a IT špecialistov. Keď je využívaná infraštruktúru ako služba (IaaS), čo zodpovedá predpečenej zmrazenej pizze, základná vrstva je už pre používateľa hotová. Musí ju upiecť a môže podľa chuti pridať šalát a nápoje a za tieto veci je aj zodpovedný. Keď sa využíva platformu ako služba (PaaS), čo zodpovedá donáške pizze, za používateľa je už urobených ešte viac rozhodnutí a služba sa využije iba ako súčasť vývoja celkového riešenia. Pri využití softvéru ako služba (SaaS), čo je prípad reštaurácie, sa zdá, že všetko je pre používateľa už hotové. Nie je tomu však tak. Používateľ má stále zodpovednosť za bezpečné stravovanie a reštaurácia nie je zodpovedná za to, že sa pri jedle dusí. V cloudovej službe SaaS to do značnej miery spočíva v manažovaní riadenia prístupu. Realita cloud computingu je o niečo

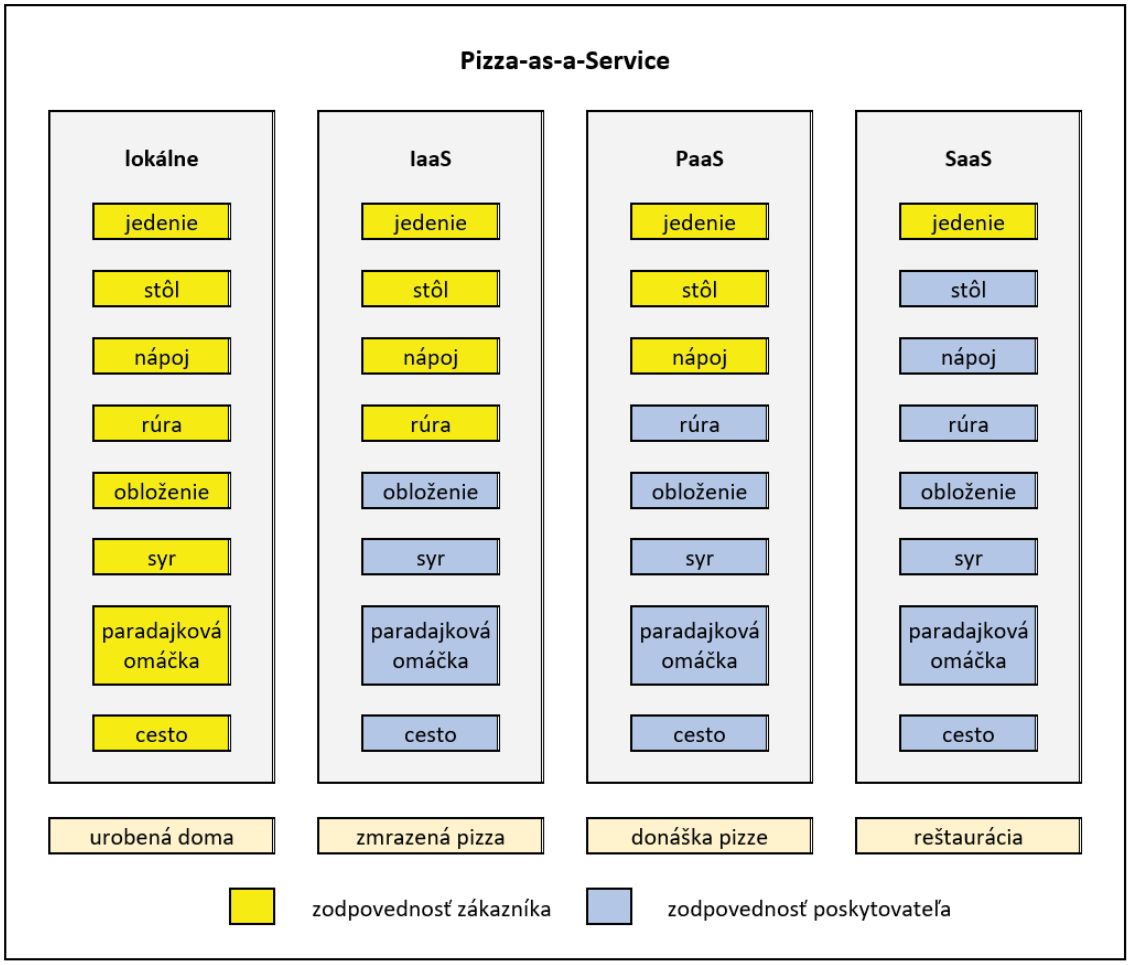
kompliKovanejšia ako analógia s pizzou, takže existuje niekoľko šedých, prekrývajúcich sa oblastí.

Poskytovateľ cloudu nesie plnú zodpovednosť za bezpečnosť fyzickej infraštruktúry, čo často zahŕňa opatrenia nad rámec opatrení aké vedia urobiť spoločností vo svojich lokálnych priestoroch. Takýmito opatreniami sú napríklad biometrická kontrola, vrátnik/bezpečnostná služba, vstupné turnikety, senzory, kamerový systém a iné opatrenia na zabránenie neoprávneným osobám prístupu k fyzickým zariadeniam. Obdobne, ak poskytovateľ ponúka virtualizované prostredia, je jeho zodpovednosťou zabezpečiť kontrolu bezpečnosti virtualizovanej infraštruktúry a udržiavať virtuálne prostredie zákazníka oddelené od virtuálnych prostredí ostatných zákazníkov. Keď sa začiatkom roku 2018 objavili chyby zabezpečenia Spectre a Meltdown, jedným z možných útokov bola možnosť, že používatelia jedného virtuálneho počítača mohli čítať pamäť iného virtuálneho počítača, ak tieto virtuálne počítače fungovali na rovnakom fyzickom počítači. Pre zákazníkov modelu IaaS bola oprava takejto zraniteľnosti v zodpovednosti poskytovateľa cloudu, avšak oprava zraniteľností v rámci operačného systému bola už zodpovednosťou zákazníka.

Zabezpečenie siete je pri IaaS brané ako zdieľaná zodpovednosť poskytovateľa a zákazníka. Existuje niekoľko vrstiev pri tvorbe siete a zodpovednosť za každú leží na inej strane. Poskytovateľ cloudu má svoju vlastnú sieť, za ktorú je zodpovedný, ale zvyčajne je nad ňou ešte virtuálna sieť (napríklad niektorí poskytovatelia cloudu ponúkajú virtuálny privátny cloud, viac v časti Virtuálny privátny cloud) a je zodpovednosťou zákazníka udržiavať danú oblasť v primeranej bezpečnostnej kondícii a zaviesť správne pravidlá na kontrolu prístupu medzi týmito vrstvami. Rôzne implementácie využívajú aj prekrývajúce sa siete, brány firewallu a šifrovanie prenosu, za čo je zodpovedný zákazník.

Za bezpečnosť operačného systému je pri IaaS obvykle zodpovedný zákazník. Ak si zákazník kupuje od poskytovateľa platformu alebo softvérové služby, zodpovednosť je na poskytovateľovi a vo všeobecnosti platí, že zákazník nemá prístup k príslušnému operačnému systému v službe. Ak tomu tak nie je, zvyčajne je zodpovednosť pridelená zákazníkovi. Middleware je v tomto kontexte všeobecný názov pre softvér, akým sú databázy, aplikačné servery alebo frontové systémy. Tvorí vrstvu medzi operačným systémom a aplikáciou – nepoužívajú ich priamo koncoví užívatelia, ale používajú sa na vývoj riešení pre koncových používateľov. Ak zákazník používa PaaS, zabezpečenie middlewaru je často spoločnou zodpovednosťou zákazníka a poskytovateľa, napr. poskytovateľ môže aktualizovať softvér, ale zákazník si ponechá zodpovednosť za nastavenia týkajúce sa zabezpečenia, akým je šifrovanie.

Aplikačná vrstva je to, čo koncový používateľ skutočne používa. Pri používaní modelu SaaS je za zraniteľné miesta v tejto vrstve (napríklad útoky typu cross-site scripting alebo SQL injection) zodpovedný poskytovateľ. Aj keď majú všetky ostatné vrstvy bezchybnú bezpečnosť, zraniteľnosť bezpečnosti v aplikačnej vrstve môže ľahko odhaliť útočníkovi zákazníkove údaje [D19].



Obrázok 0-3 Pizza as a Service [D19].

Ako posledná je bezpečnosť prístupu k údajom. Za tú je takmer vždy zodpovedný zákazník. Ak poskytovateľovi cloudu nesprávne oznámi, aby povolil prístup k údajom, napríklad udelenie nesprávnych oprávnení na prístup k úložisku, k middlewaru alebo k SaaS, zodpovednosť za takto nesprávne pridelené oprávnenia nenesie poskytovateľ, ale zákazník, Obrázok 0-1.

Hlavnou príčinou mnohých bezpečnostných incidentov je predpoklad zákazníka, že poskytovateľ cloudu má zodpovednosť za všetko a aj za časti systému, ktoré spadajú pod zákazníkovu zodpovednosť. Príkladom bezpečnostných incidentov v reálnom svete, ktoré pramenia z nesprávneho pochopenia modelu zdieľanej zodpovednosti, môže byť používanie služby Amazon Web Services Simple Storage (AWS S3). Uistenie sa, že úložisko AWS S3 je bezpečné a šifrované, nepomôže pri ochrane údajov, ak nie je správne nastavená kontrola prístupu a do úložiska dostanú od organizácie prístup aj neoprávnené osoby. Model zdieľanej zodpovednosti v cloude nie je stále medzi podnikmi dostatočne známy a pochopený. IT manažéri sa častokrát pri vytváraní bezpečnostných rozhodnutí nesprávne domnievajú, že poskytovatelia cloudových služieb sú zodpovední za zabezpečenie zákazníckych údajov v cloude. Navyše sa domnievajú, že títo poskytovatelia sú zodpovední aj za zabezpečenie zákazníckych aplikácií. Preto je

potrebné si pri využívaní cloudu naštudovať podmienky uvedené v zmluve a zamerať sa na otázku zodpovednosti za jednotlivé úlohy v cloude [D19].

Modely zavádzania cloud computingu

Základné modely cloudových služieb diskutované v predchádzajúcej časti sa zameriavajú na splnenie požiadaviek zákazníkov na rôznych úrovniach riadenia výpočtového hardvéru a softvéru. Výber typu cloudovej služby má priamy vzťah s veľkosťou organizácie. Na základe toho, kde je cloud nasadený a kým, a kto ho vlastní a spravuje, ako aj podľa toho kto sú jeho hlavní používatelia, sú cloudy rozdelené do piatich kategórií: *verejný cloud*, *privátny cloud*, *virtuálny privátny cloud*, *komunitný cloud* a *hybridný cloud* [MB16].

Verejný cloud

Verejný cloud je najbežnejšou a najznámejšou formou cloudu a je otvorený pre použitie pre všetkých – pre podnikanie, priemysel, vládne inštitúcie, neziskové organizácie a aj jednotlivcov. Cloudovú infraštruktúru však vlastní a riadi poskytovateľ cloudových služieb – organizácia poskytujúca cloudové služby. Verejné cloudové služby sa ponúkajú na základe modelu platby za použitie (pay-as-you-go), t. j. zákazník platí len za zdroje, ktoré skutočne použil a nemá vopred určený ich počet a kapacitu. Niektoré aplikácie vo verejných cloudoch sú prístupné zadarmo.

Verejný cloud poskytuje služby každému, kto má prístup na internet. Takáto služba sa môže poskytovať pomocou výpočtových zdrojov umiestnených kdekoľvek vo svete. Verejný cloud je použiteľný na rôznych úrovniach abstrakcie. Je možné nájsť verejné cloudy, ktoré poskytujú infraštruktúru, platformu, softvér, informácie alebo obchodné procesy ako službu. Malé a stredné podniky zvyčajne používajú verejný cloud ako svoj primárny výpočtový zdroj. Veľké korporácie používajú verejný cloud ako doplnok k svojim interným výpočtovým zdrojom. Výhodou cloud computingu je jeho schopnosť poskytovať výpočtové a úložné služby podľa potreby. Náklady na verejný cloud sú relatívne nižšie ako na súkromné cloud. Malé a stredné podniky sú schopné si vyčleniť finančný obnos na základný výpočtový hardvér a softvér vo verejnom cloude, čo odbremeňuje podnik od záťaže budovať vlastné IT oddelenie. Podnik môže podľa potreby využívať potrebné výpočtové a úložné zdroje verejného cloudu a platiť len za to, čo skutočne využil. Verejný cloud môže byť riešením aj pre veľké organizácie, ktoré nezamýšľajú investovať do vlastnej IT infraštruktúry, ale ktoré pociťujú prudký nárast dát a potrebu ich spracovania. Dátové centrá sú kľúčom k úspechu veľkých organizácií a požiadavky na ukladanie údajov v dátových centrách je možné riešiť práve pomocou verejného cloudu.

Ďalšou výhodou verejného cloudu je jednoduchosť používania. Organizácie, ktoré potrebujú počítačové služby od poskytovateľa verejných cloudových služieb, sa môžu ľahko zaregistrovať pre využívanie cloudu online. Poskytovateľ formou pay-as-you-go ponúka hardvérové aj softvérové zdroje, ktoré zákazník potrebuje, prideľovanie

a odoberanie zdrojov je robené automatizovane. Služba je k dispozícii spoľahlivo na báze 24/7.

Nevýhodou verejného cloudu je bezpečnosť údajov a niektoré, predovšetkým štátne organizácie ho nesmú využívať z regulačných dôvodov. Napríklad spoločnosti so sídlom v USA nemajú dovolené ukladať údaje o spotrebiteľoch v iných krajinách. Je faktom, že verejné cloudy na jednom fyzickom serveri pomocou virtualizácie poskytujú zdroje naraz viacerým zákazníkom. Z toho vychádza aj obava zákazníkov, že nedostatok kontroly nad hardvérom, ako aj možnosť prístupu niekoho iného k ich dátam, môže narušiť bezpečnosť ich údajov. Ďalšou nevýhodou je spôsob prístupu. Prístup k verejnému cloudu je prostredníctvom internetového pripojenia a zákazníci sú obmedzení rýchlosťou, ktorú dostanú prostredníctvom svojho poskytovateľa internetových služieb. Prístup k službe cloudu odvšadiaľ, kde je internetové pripojenie je však aj jeho hlavnou výhodou. Inou nevýhodou pre organizácie je napríklad aj nemožnosť odpisovať akékoľvek počítačové prostriedky, pretože organizácia nevlastní svoju infraštruktúru. Výsledkom je, že niektoré veľké spoločnosti uprednostňujú privátne cloudy [GJ18].

Rovnako je v súčasnosti pre organizáciu náročné vykonať migráciu k inému poskytovateľovi kvôli nedostatku štandardov [S14]. V dôsledku toho bude mať každý zákazník migrujúci od jedného cloudového poskytovateľa k inému zrejme ťažkosti s použiteľnosťou svojich údajov z dôvodu rozdielnych formátov úložiska. Problém to môže spôsobovať predovšetkým malým podnikom, ktoré majú tendenciu používať model SaaS viac ako PaaS a IaaS. Stredné a veľké organizácie, ktoré používajú PaaS a IaaS, majú vyššiu úroveň kontroly nad aspektmi ukladania, takže prechod na iného poskytovateľa cloudu nie je až taký zložitý. Celkovo výhody, ktoré verejný cloud ponúka, prevažujú nad niektorými z vyššie uvedených nevýhod.

Medzi príklady verejnej cloudovej služby patria okrem iného Google Print, Dokumenty Google, Microsoft Office 365, Amazon EC2 a Amazon Cloud Player.

Privátny cloud

Privátny cloud, alebo aj interné cloudové úložisko, je nasadený, poskytovaný a kontrolovaný organizáciou, ktorá ho pre jej vlastné použitie aj vlastní, a je zväčša oddelený od verejnej siete prostredníctvom firewallu. Niektoré organizácie odmietajú používať verejné cloudy. K tomuto ich vedú obavy spojené s bezpečnosťou verejných cloudov a obava o súkromie údajov uložených na verejných cloudoch, alebo aj nesúhlas so stanovenými požiadavkami a predpismi pri používaní verejných cloudov, ktoré stanovil cloudový poskytovateľ. A preto nasadia vlastné prostredie cloud computingu pre svoje výhradné použitie, prípadne ho poskytnú aj svojim obchodným partnerom. V takomto prostredí majú väčšiu kontrolu používania cloudu. Cloudové služby sa poskytujú z vlastnej súkromnej siete. Za obmedzených okolností sa privátne cloudové služby môžu poskytovať aj prostredníctvom internetu, avšak s obmedzeniami prístupu, aby k službám privátneho cloudu mohli pristupovať iba oprávnené subjekty, pričom sa často využívajú virtuálne privátne siete (VPN, Virtual Private Network).

Tým, že organizácia má vlastný privátny cloud, získava prevádzkovú efektívnosť, efektívne využíva svoje existujúce zdroje, a má plnú kontrolu nad cloudom, aplikáciami a údajmi v cloude. Na druhej strane musí znášať všetky náklady spojené s údržbou cloudu, modernizáciou jeho technického vybavenia a prípadnými bezpečnostnými problémami. V porovnaní s verejným cloudom je to nákladná služba. Privátne cloudy si zvyčajne môžu dovoliť iba veľké spoločnosti, a to jednak z pohľadu budovania infraštruktúry, ako aj z pohľadu riadenia systému.

Existujú štyri základné typy privátnych cloudov. V klasickom privátnom cloude organizácia prevádzkuje cloud v jednom zo svojich dátových centier za firemným firewallom. Architektúra sa podobá na intranet, pri ktorom organizácia využíva techniky internetu, ale obmedzuje prístup k obsahu iba pre interných zamestnancov. V tomto prípade organizácia využíva technológiu cloud, ale obmedzuje používateľov na svojich interných zamestnancov. Druhý typ súkromného cloudu je privátny cloud, ktorý spravuje poskytovateľ tretej strany. V tomto prípade organizácia stále vlastní infraštruktúru v jednom zo svojich dátových stredísk, ale správa zariadenia je v rukách tretej strany. Ide o tzv. „spravovaný privátny cloud“, čo znamená, že infraštruktúra patrí organizácii, ale spravuje ju niekto iný. V treťom modeli označenom ako *hosťovaný privátny cloud* poskytuje poskytovateľ cloudových služieb potrebnú infraštruktúru a spravuje ju. Prínosom pre zákazníka je v tom, že škálovateľnosť, elasticita dopytu a dostupnosť sú zaručené poskytovateľom cloudových služieb a pretože servery nie sú zdieľané s inými organizáciami, je tu aj vyššia bezpečnosť. Štvrtým modelom je virtuálny privátny cloud, ktorý je uvedený nižšie ako samostatný model.

Pri použití privátneho cloudu sa niektoré z výhod cloud computingu stratia, pretože organizácia musí investovať do infraštruktúry. Navyše dostupnosť infraštruktúry sa nezvyšuje tak rýchlo ako v skutočnom cloude. Použitie výrazu „cloud“ pri privátnom cloude je opodstatnené používaním cloudových konceptov, ako je napr. virtualizácia. Organizácia využívajúca privátny cloud teda najprv prebuduje infraštruktúru s ohľadom na očakávaný dopyt a udržiava ju za firemným firewallom. Prístup je obmedzený na zamestnancov organizácie. Pretože organizácia riadi infraštruktúru aj prístup k systémom, je schopná lepšie vyhovieť interným požiadavkám a mať vyššiu úroveň bezpečnosti ako vo verejnom cloude. Aby bola organizácia schopná riadiť privátny cloud, potrebuje značné množstvo IT pracovníkov, ktorí sa venujú iba správe privátneho cloudu. Príkladom takýchto súkromných používateľov cloudu sú veľké organizácie ako IBM, Cisco a Verizon [B17, S14].

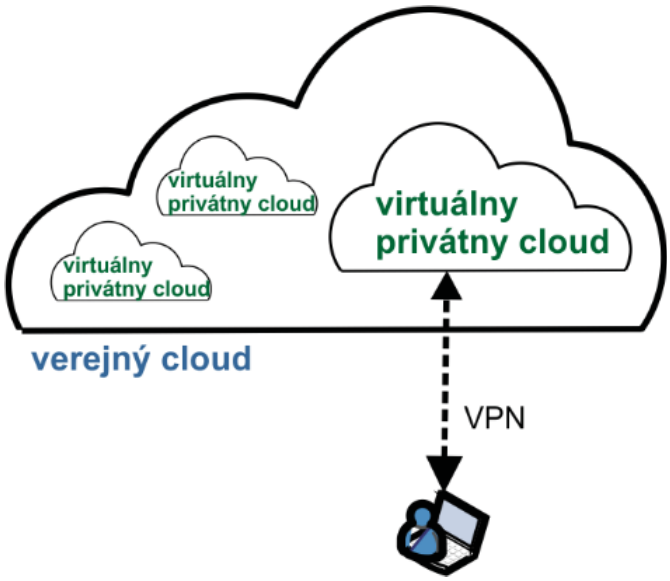
Príkladom osobného privátneho cloudu [R15] môže byť privátny cloud v rodinnom dome prostredníctvom siete LAN. Používatelia cloudu v dome môžu cloud využívať napríklad na (i) pripájanie streamovacieho serveru k set-top boxu s videom, takže videá je možné sledovať, nahrávať alebo prehrávať odkiaľkoľvek v dome; (ii) poskytovanie záložného servera na centrálne ukladanie súborov; (3) synchronizačnú službu, ktorá synchronizuje údaje medzi zariadeniami (notebooky, mobilné telefóny, tablety atď.) pomocou bezdrôtovej siete LAN.

Vo všeobecnosti pri privátnom cloude je organizácia, ktorá spravuje dátové centrum, schopná sama naplno využívať veľké množstvo úložného a výpočtového výkonu vyhradeného iba pre seba. Privátny cloud umožňuje veľkej organizácii zvládnuť elasticitu dopytu po výpočtoch pomocou virtualizácie serverov a efektívnejšie zužitkovávať ich kapacitu, ktorá je často nevyužitá. V prípade skladovania údajov však musí poskytovateľ privátneho cloudu investovať do hardvéru len pre tento účel. Práve pri veľkých organizáciách je nastolený trend, že budujú vlastné úložné centrá predovšetkým kvôli ochrane svojich údajov. Preto musí organizácia dôsledne zvážiť, či pre jej potreby a predpokladané náklady je alebo nie je práve privátny cloud správnym riešením [FH17].

Virtuálny privátny cloud

Virtuálny privátny cloud je segment verejného cloudu, ktorý je špeciálne určený pre vytvorenie izolovaného prostredia od ostatných používateľov tak, aby vyhovel požiadavkám používateľa na bezpečnosť. Virtuálne privátne cloudy oproti verejným cloudom poskytujú používateľom väčšiu kontrolu nad používanými zdrojmi.

Hlavný rozdiel spočíva v tom, že zatiaľ čo je privátny cloud prevádzkovaný prostredníctvom vnútornej infraštruktúry organizácie, virtuálny privátny cloud využíva infraštruktúru poskytovateľa cloudových služieb tretích strán. Na rozdiel od verejného cloudu, ktorý obsluhuje viac organizácií, však virtuálny privátny cloud zostáva vyhradené pre jednu organizáciu, Obrázok 0-4.



Obrázok 0-4 Virtuálny privátny cloud.

Poskytovateľ cloudových služieb pri virtuálnom privátnom cloude poskytuje svojim zákazníkom virtuálne servery s prístupom VPN (Virtual Private Network). Táto služba je oveľa lacnejšia v porovnaní s predchádzajúcim čisto privátnym cloudom, ale je drahšia ako verejný cloud. Zákazníci, ktorí si vyberú virtuálny privátny cloud, by mali používať

cloudovú službu typu IaaS, pretože v takom prípade by riadili všetky nastavenia na svojich virtuálnych serveroch. Pretože prístup k ich virtuálnym serverom je cez VPN, dostávajú vyššiu úroveň bezpečnosti ako vo verejnom cloude. V tomto prípade je tretia strana poskytovateľom cloudových služieb so všetkými výhodami cloudovej služby, ako je škálovateľnosť, elasticita dopytu, dostupnosť a skladovanie. Poskytovateľmi virtuálneho privátneho cloudu sú zväčša poskytovatelia IaaS ako Amazon VPC, VMware, Microsoft Private Cloud, IBM Cloud Private, Google Virtual Private Cloud a Alibaba Virtual Private Cloud [GJ18, S14].

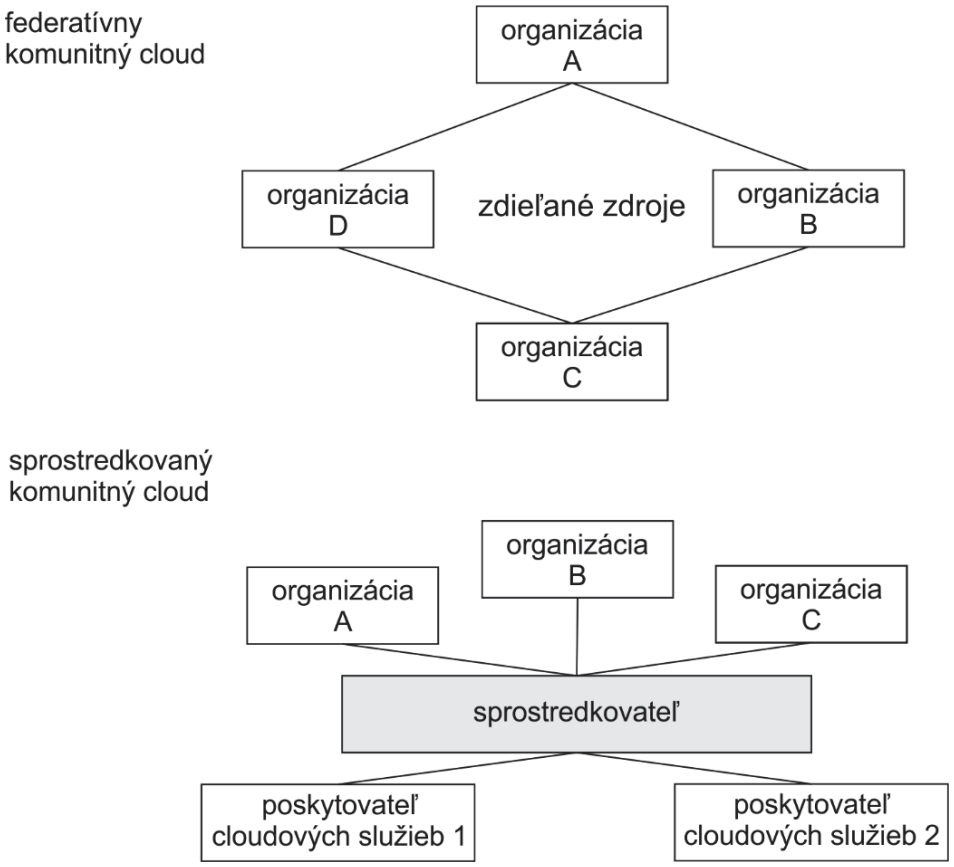
Komunitný cloud

Komunitný cloud je širšou verziou privátneho cloudu. Je optimalizovaný a špeciálne nasadený na použitie v určitom priemyselnom odvetví alebo skupine používateľov so spoločným záujmom tak, aby spĺňal konkrétne požiadavky na riešenie ich kľúčových problémov. Z tohto dôvodu môže niekoľko subjektov združiť svoje zdroje na vytvorenie spoločného komunitného cloudu. Ak ide o IaaS komunitný cloud, komunitný cloud zdieľa rovnakú cloudovú infraštruktúru, ak ide o SaaS komunitný cloud, zdieľa rovnaký cloudový softvér, alebo zdieľa rovnaké podnikové procesy v cloude, ak ide o BPaaS (Business Process as a Service) komunitný cloud. Na rozdiel od privátneho cloudu sú zvyčajne komunitné cloudové služby poskytované prostredníctvom internetu.

Koncepcia komunitného cloudu sa vyvinula, keď si podniky v určitom odvetví, ako napr. automobilový priemysel, energetika, financie a zdravotníctvo, uvedomili, že potrebujú špecializované aplikácie, ktoré iné odvetvia nevyužívajú. Komunitný cloud ponúka výhody verejného cloud computingu, ale obmedzuje sa na konkrétny priemyselný segment a bezpečnostné funkcie hosťovaného privátneho cloudu. Napríklad v bankovom sektore, banka sprístupňuje dôvernú komunikáciu s klientami iba prostredníctvom svojej siete, do ktorej sa musí zákazník prihlásiť. Banka však môže upozorniť zákazníka na dostupnú komunikáciu prostredníctvom verejného e-mailového systému, ako je napr. Gmail.

Existujú dva základné typy komunitných cloudových modelov – *federatívny* a *sprostredkovaný*, Obrázok 0-5. Základným predpokladom je, že organizácie v danom sektore sa zúčastňujú iba na tomto type cloudu. Vo federatívnom modeli komunitného cloudu, kde spoločnosti nejakého sektora vytvorili komunitný cloud a poskytli do neho svoje výpočtové zdroje, je akýkoľvek poskytnutý nepoužitý výpočtový prostriedok jednej organizácie na požiadanie poskytnutý inej členskej organizácii. V sprostredkovanom modeli vystupuje dôveryhodná tretia strana ako sprostredkovateľ a rozhranie pre členov komunitného cloudu. Sprostredkovateľ je zodpovedný za zaobstaranie rôznych služieb potrebných v priemyselnom sektore a za ich sprístupnenie všetkým členom.

Komunitný cloud je uzavretý systém, ktorý je k dispozícii iba pre členské organizácie. Hlavným prínosom pre organizácie využívajúce komunitný cloud je to, že majú väčšie úspory nákladov pri používaní aplikácií potrebných v ich sektore. Model sprostredkovateľa podporuje túto funkciu lepšie ako federatívny model [B17, S14].



Obrázok 0-5 Federatívny a sprostredkovaný komunitný cloud

Výhodou modelu federatívneho komunitného cloudu je zdieľanie výpočtových zdrojov členských organizácií, keď sú nečinné. Avšak neriešia sa tu otázky zodpovednosti s takýmto zdieľaným spracovaním, čo je problém, najmä ak dôjde k výpadku služby uprostred spracovania a služba sa vykonávala na výpočtových zdrojoch inej organizácie. Ďalšou otvorenou otázkou je zodpovednosť členskej organizácie za udržiavanie systému a za to, či a ako sa bude platiť časový podiel v cloude. Model sprostredkovania v komunitnom cloude je oveľa prehľadnejší a to aj pri riešení otázok zodpovednosti. Sprostredkovateľ je zodpovedný za urovnanie zmlúv s poskytovateľmi zdrojov, poskytuje členom potrebnú dôveru na používanie systému a riešenie sporov. Členovia komunitného cloudu so sprostredkovateľom sa nemusia zaujímať o aspekty bezpečnosti, pretože aj túto otázku rieši sám sprostredkovateľ. Sprostredkovateľ je navyše schopný poskytovať aj ďalšie špecifické služby.

Príkladom komunitných typov cloudov sú napr. *OpenCirrus*[5], čo je testovacie centrum pre výskum určené pre univerzity a výskumné inštitúcie a *Asite Solutions*[6] špeciálne navrhnutý pre stavebníctvo.

[5] https://opencirrus.org/
[6] https://www.asite.com/

Hybridný cloud

Hybridný cloud je kombináciou dvoch alebo viacerých vyššie uvedených cloudových modelov. Typickým použitím v tomto modeli je kombinácia verejného aj privátneho cloudu. Pre nasadenie svojich menej kritických služieb s nízkym rizikom využíva organizácia verejný cloud a kritické aplikácie a údaje organizácie si organizácia spracováva vo svojom internom privátnom cloude. Hybridný model tak umožňuje selektívnu implementáciu, ktorá rieši obavy o bezpečnosť a stratu kontroly. Na druhej strane umožňuje využívať aj výhody verejných cloudov, ktoré ponúkajú nižšie nákladové výdaje, viac aplikačných možností, ako aj rôzne výpočtové zdroje.

Hybridný cloud zväčša využíva na vybudovanie časti verejného cloudu model IaaS. Keďže organizácia riadi používanie infraštruktúry v cloude, má úplnú slobodu pri presúvaní aplikácií medzi jednotlivými oblasťami. Hybridný cloud vďaka tomu, že má v architektúre súčasť verejného cloudu, ponúka aj cloudové výhody verejného cloudu ako sú škálovateľnosť, dostupnosť, pružnosť dopytu a model pay-as-you-go. Hybridný cloud je vhodný pre veľké podniky alebo špecializované organizácie s výpočtovo náročným systémom, ktorý využíva výpočtové zdroje nárazovo. Hybridné cloudové služby poskytujú všetci hlavní poskytovatelia cloudových služieb, ako sú Amazon, VMware, Google, Azure, či HP [S14].

Organizácia ocení výhody nasadenia hybridného cloudu napríklad v prípadoch, keď sa objavia nové aplikácie, ktoré potrebuje pred ich začlenením do svojich systémov otestovať, či budú a ako súčinné s jej už existujúcimi procesmi. Z tohto dôvodu by hybridná cloudová správa mala byť rozšírením privátnej cloudovej správy, aby organizácia mohla bez problémov presúvať aplikácie medzi dvoma časťami hybridného cloudu. Ďalšou z výhod hybridného cloudu je schopnosť organizácie udržať istý stupeň bezpečnosti, aj keď zmiešaný prístup vedie organizáciu vzdať sa určitej kontroly nad svojimi IT prostriedkami. Nevýhody si hybridný cloud preberá od verejného cloudu, ktorý je jeho súčasťou. Ide predovšetkým o problémy s jurisdikciou, pretože poskytovateľ cloudu v jednej jurisdikcii nemusí poznať právne požiadavky v inej krajine alebo regióne. Bezpečnostné požiadavky poskytovateľa verejného cloudu tiež nemusia byť v súlade s vnútornými predpismi organizácie.

Hybridný cloud sa používa aj v prípade, keď cloudová služba jedného cloudu potrebuje využívať výpočtové zdroje z iných cloudov, pretože jej vlastné sú využité na plnú kapacitu. Poskytovatelia cloudu k tomuto často pristupujú z dôvodu, aby splnili svoje záväzky o úrovni služieb [GJ18].

Okrem vyššie zmienených poskytovateľov hybridných cloudov, je možné hybridný cloud vytvárať aj prostredníctvom open source softvéru, ako je napr. nástroj Eukalyptus[7], či OpenStack[8].

[7] https://www.eucalyptus.cloud/
[8] https://www.openstack.org/enterprise/

Cloudové úložisko

V predchádzajúcej kapitole sú uvedené tri základné modely cloudových služieb – SaaS, PaaS a IaaS. Cloud je však v mnohých organizáciách využívaný hlavne na ukladanie dát. Pri ukladaní v cloude sa údaje ukladajú na viacerých serveroch tretích strán a nie len na určených serveroch pre daného používateľa ako je tomu v tradičnom sieťovom úložisku; používateľ pristupuje k virtuálnemu úložisku. Skutočné umiestnenie úložiska sa môže meniť podľa toho ako cloud dynamicky spravuje dostupný úložný priestor. Používatelia však pre svoje dáta uvidia vždy statické umiestnenie. Kľúčovými výhodami cloudového úložiska sú znížené náklady a lepšia zálohovacia bezpečnosť a dostupnosť údajov. Virtuálne prostriedky v cloude sú zvyčajne lacnejšie ako konkrétne fyzické zdroje pripojené k lokálnemu počítaču alebo sieti. Dáta uložené v cloude sú všeobecne bezpečné proti náhodnému vymazaniu alebo zlyhaniu pevného disku, pretože poskytovatelia cloudových služieb uchovávajú viac kópií údajov na viacerých fyzických zariadeniach. Ak dôjde k zlyhaniu jedného počítača, údaje, ktoré boli na tomto počítači, sa dajú získať z iných počítačov v cloude. Poskytovatelia cloudu vo všeobecnosti ponúkajú lepšie bezpečnostné opatrenia, ako si môže dovoliť malý podnik. Ukladanie podnikových údajov v cloude však vyvoláva určité obavy ohľadom bezpečnosti a súkromia [MB16]. Hlavnými komerčných poskytovateľmi cloudových úložísk sú Apple iCloud, Dropbox, Disk Google, Microsoft OneDrive a Amazon S3.

Cloudové úložisko slúži pre mnohé organizácie na dva účely. Po prvé, organizácie musia zálohovať údaje a na tento účel je hospodárne používať práve cloud. Navyše, dáta sú uložené v šifrovanej forme, čím organizácii poskytuje potrebnú bezpečnostnú ochranu. Pretože zálohovanie údajov je potrebné len na určité časové obdobie, organizácia uzatvorí zmluvu o poskytnutí služby/úložiska na určité množstvo ukladacieho priestoru, napríklad 1 TB, a podľa potreby opätovne používa tento odkladací priestor. Keďže využíva tento priestor na zálohovanie údajov, nie je potrebné nepretržite pristupovať k uloženým údajom. Toto je najpoužívanejší typ úložnej služby v cloude využívaný organizáciou najmä na možnosť obnovy údajov po havárii, preventívnu ochranu uložením údajov mimo lokality umiestnenia organizácie alebo na ich archiváciu.

Druhé využitie cloudového úložiska je ukladanie v reálnom čase. V tomto prípade musí organizácia brať do úvahy rýchlosť čítania a zápisu dát poskytovateľa cloudu. Typická latencia pre uloženie dát na lokálne disky je 5 ms. Organizácia teda použije lokálne úložisko pre údaje, ktoré sú často potrebné a k ich prístupu je potrebná nízka latencia. Ostatné typy údajov, ktoré by mohli tolerovať strednú až vysokú latenciu, napríklad 25 až 100 ms, sa presunú do cloudu. Vyššia latencia je v cloude z dôvodum že sa k dátam pristupuje cez Internet, kde využívané smerovače a prepínače majú určité vlastné oneskorenia. Z týchto dôvodov sa miera latencie 100 ms nepovažuje za vysokú [S14]. Na druhej strane, cloudové spoločnosti ako Amazon a Google účtujú zvyčajne len niekoľko centov za gigabajt úložného priestoru mesačne za štandardné úložisko. Navyše, keďže spoločnosť vie predvídať potrebné množstvo úložného priestoru, môže si u poskytovateľa cloudu objednať potrebné množstvo úložného priestoru na dlhšie časové obdobie,

napríklad jeden rok, s nižšími nákladmi, ako sú bežné náklady. Hybridný prístup k ukladaniu údajov sa stáva čoraz obľúbenejším v prípadoch, keď spoločnosť ukladá najčastejšie používané údaje na lokálne úložisko a ostatné údaje do cloudu.

Na zlepšenie výkonnosti ukladania poskytovateľov cloudových služieb sa používa koncept deduplikácie. Deduplikácia znamená, že je uložená iba jedna kópia údajov a všetky ostatné aplikácie, ktoré vyžadujú rovnaké údaje, smerujú do oblasti kde sú údaje uložené. Deduplikácia je veľmi užitočná v e-mailových aplikáciách, keď je priložený súbor distribuovaný viacerým používateľom prostredníctvom e-mailu. Deduplikácia namiesto ukladania prílohy do každej doručenej pošty umožňuje, aby sa jedna kópia súboru uložila do spoločného úložného priestoru a všetky Inboxy, ktoré tento súbor potrebujú, jednoducho ukážu na tento spoločný úložný priestor. Služba úložiska v cloude tak poskytuje nielen základné úložisko, ale tiež efektívne úložisko [B17].

Výhody, limity, výber cloudu

Cloud computing ponúka svojim používateľom množstvo podstatných výhod. Má však aj svoje obmedzenia, ako aj určité riziká, ktoré závisia od typu jeho využitia. Preto je potrebné, aby organizácia či používateľ pri výbere a nasadzovaní cloud computingu poznali, pochopili a riešili možné obmedzenia a riziká vyplývajúce z jeho implementácie.

Výhody využívania cloudu v organizácii

Medzi hlavné výhody cloud computingu patria znížené kapitálových a prevádzkových nákladov, zvýšená flexibilita, škálovateľnosť na požiadanie, ľahšie a rýchlejšie nasadenie aplikácií, jednoduché použitie a dostupnosť obrovských cloudových zdrojov pre všetky druhy aplikácií alebo iné použitie. Mnoho aplikácií, vrátane e-mailov, tvorby a správy kancelárskych dokumentov, ukladania veľkého množstva dát, sa čoraz viac presúva do cloudov a využíva výhody tejto novej IT paradigmy.

Cloud computing oslobodzuje používateľov a organizácie od obmedzení lokálnych výpočtových zdrojov a umožňuje im prístup k obrovským výpočtovým zdrojom v cloude. Aby používatelia mohli cloudové zdroje využívať odkiaľkoľvek a kedykoľvek, stačí im iba pripojenie na internet a webový prehľadávač. Okrem bežných aplikácií umožňuje cloud používateľom spúšťať aj výpočtovo náročné aplikácie, alebo aplikácie náročné na množstvo uložených dát, keďže výpočtové a úložné zdroje sú získavané priamo z cloudu.

Verejné cloudy eliminujú nemalé kapitálové výdavky na hardvér a počiatočné licenčné poplatky za softvér, ako aj činnosti spojené s údržbou hardvéru a softvéru a jeho aktualizáciou. Cloudové aplikácie môžu byť nasadené súčasne tisícom používateľov na rôznych miestach po celom svete a môžu byť pravidelne ľahko aktualizované. Keďže cloudy poskytujú lepšiu kontinuitu podnikania a bezpečnosť údajov, sú obzvlášť atraktívne pre malé a stredné podniky, ako aj pre organizácie v oblastiach náchylných na katastrofy. Startupy a vývojári aplikácií môžu využiť cloud computing na vyskúšanie svojich nápadov bez toho, aby museli investovať do svojej vlastnej infraštruktúry [MB16].

Organizácie zavádzajú využívanie cloud computing predovšetkým preto, aby mohli naň preniesť všetky svoje problémy spojené so správou informačného systému. Z hľadiska malých a stredných podnikov zvyšuje schopnosť podniku sústrediť sa na svoje podstatné silné stránky a využívať všetky výhody dostupnosti informačného systému bez nutnosti budovať vlastnú IT infraštruktúru. S tým úzko súvisí otázka stálej dostupnosti cloudových systémov, čo v dnešných podmienkach znamená dostupnosť 24/7. Zákazníci očakávajú, že cloud bude k dispozícii takmer nepretržite. Keď spoločnosť prevádzkuje svoj vlastný informačný systém, na jeho nepretržitú prevádzku musí vynaložiť značné finančné zdroje. Navyše, každý týždeň musí vykonávať zálohu a údržbu systému, kedy je zvyčajne systém mimo prevádzky. Keď sa však služba presunie do cloudu, používateľ neočakáva výpadky systému. Cloudové spoločnosti sa usilujú pre svoju cloudovú službu o dostupnosť 99,99% systémového času. Výpadky tak predstavujú odstávku systému maximálne 8 sekúnd za deň. Aby sa zaručila taká vysoká prevádzková dostupnosť, poskytovatelia cloudových služieb musia výrazne investovať do redundancie zdrojov a automatizácie prideľovania služieb. Ak dôjde k výpadku výpočtového systému jednej lokálnej organizácie, ovplyvní to iba jednu organizáciu a jej zákazníkov, čo zvyčajne nie je veľký počet. Ale ak dôjde k výpadku systému poskytovateľa cloudových služieb, ktorý slúži mnohým zákazníkom, výpadok má oveľa väčší dopad. Ako už bolo uvedené, cloudový poskytovatelia sa snažia tomu zabrániť redundanciou t. j. vytváraním kópií údajov, systémov a zariadení, takže ak dôjde k poškodeniu alebo nedostupnosti cloudovej služby, je okamžitý a bezpečný prístup k zálohovaným verziám [S14].

Ďalšou veľkou výhodou cloud computingu je jeho schopnosť poskytovať neobmedzenú kapacitu servera, označovanú aj ako pružnosť služieb alebo elasticita dopytu. Cloudové spoločnosti navrhujú svoj systém pomocou konceptu virtualizácie, čím umožňujú sprístupnenie serverov bez obmedzenia. Virtualizácia znamená, že jedno fyzické zariadenie je rozdelené do viacerých virtuálnych strojov (VM) a sprístupnené zákazníkovi. Každý VM môže byť virtuálny server. Hlavné fyzické zariadenie sa nazýva „hostiteľ“ a každý virtuálny počítač sa nazýva „hosť“. Napríklad, ak každý hosť vyžaduje minimálne 2 GB úložného priestoru a ak má hostiteľ aspoň štvorjadrový procesor s najmenej 1 TB voľného miesta na pevnom disku, potom je možné na jednom hostiteľovi vytvoriť desať virtuálnych serverov, každý s pridelenou kapacitou 100 GB. Pri dnešnom pracovnom zaťažení je pridelenie 100 GB úložného priestoru malé. V skutočnosti počet virtuálnych serverov na hostiteľa závisí od typu plánovaného pracovného zaťaženia na server. Hostitelia zvyčajne prichádzajú s kapacitou najmenej 32 TB pevného disku a štyrmi viacjadrovými procesormi. Uvedený príklad ilustruje skutočnosť, že jeden hostiteľ môže poskytnúť viac serverov, pretože typické využitie servera je iba okolo 20 % jeho kapacity. Aj keď všetky servery fungujú na 50 % svojej kapacity využitia, nebude zaťaženie procesora hostiteľa príliš enormné. Pritom sa každému zákazníkovi v cloude zdá, že počet serverov, ku ktorým má prístup, je neobmedzený. Práve podniky považujú neobmedzenú dostupnosť výpočtového výkonu za dôležitý aspekt pri rozhodovaní sa používať cloud oproti vytváraniu a spravovaniu vlastného výpočtového systému. V praxi to znamená, že organizácia používajúca určité množstvo výpočtového zdroja v jenom

čase môže časť týchto zdrojov uvoľniť v inom čase, keď je jej dopyt po takomto zdroji nižší. A práve škálovateľnosť, t. j. schopnosť zvýšiť alebo znížiť potrebu výpočtových zdrojov robí cloud computing pre mnohé podniky atraktívnym a podniky majú z tejto funkcie značný úžitok [B17, S14].

Náklady sú dôležitou metrikou pre všetky podniky. Cloud computing podporuje model platby za použitie pay-as-you-go. Vzhľadom na potrebu pružnosti dopytu, umožňuje model zákazníkovi platiť len za to čo použije a neinvestovať do drahého výpočtového hardvéru, ktorý by využil len málokedy. Aj z pohľadu poskytovateľa cloudových služieb je to rentabilné z dôvodu škálovateľnosti ponúkanej služby. Navyše poskytovateľ cloudových služieb má výhodu, že si môže vybrať umiestnenie svojich serverov v regióne, kde sú náklady na elektrinu nižšie ako má zákazník. Pokrok komunikačných technológií umožňuje, že umiestnenie cloudových serverov do iného regiónu nepredstavuje žiadne obmedzenia služieb, pretože všetci zákazníci majú prístup ku cloudovej infraštruktúre cez internet. Architektúra cloudových služieb je distribuovaná aj kvôli dostupnosti, a aj kvôli spoľahlivosti. Z pohľadu zákazníka nie sú ponúkané služby viazané na ich umiestnenie. Okrem toho, je zákazník schopný na prístup ku cloudovej službe používať akékoľvek zariadenie. V porovnaní s lokálnymi výpočtovými centrami spoločností, kde je potrebné spravovať inú sadu rozhraní API, aby sa dali rovnaké informácie sprístupniť na mobilných zariadeniach, pri cloudoch poskytovatelia cloudových služieb uspokojujú potreby veľkej a rozmanitej skupiny zákazníkov a implementujú ihneď svoje služby prostredníctvom všetkých typov zariadení. Cloudové služby výrazne skracujú čas nasadenia infraštruktúry.

Organizácie, ktoré využívajú cloudové služby, majú schopnosť rýchlo meniť kombinácie služieb. Napríklad zákazník, ktorý potrebuje otestovať jednu zo svojich aplikácií na inej platforme, ako napríklad OS Mac alebo OS Linux, je schopný rýchlo získať potrebné zdroje a otestovať svoju aplikáciu. Uvedený typ agility je výhodou cloudu. Model PaaS umožňuje zákazníkovi vybrať si akúkoľvek platformu, ktorú potrebuje, aby svoje služby ponúkal alebo testoval. Dostupnosť všetkých typov zdrojov v cloude umožňuje zákazníkovi výrazne znížiť jeho kapitálové výdavky a presunúť ich na prevádzkové výdavky. Pretože všetky aspekty riadenia informačného systému pre podnikanie sú presunuté do cloudu, uvoľňujú sa interné zdroje v organizácii.

Ďalšou vysoko využívanou službou cloudu je úložisko dát. Medzi pridružené činnosti, ktoré sa v cloude realizujú spolu s úložiskom, patria zálohovanie a bezpečnosť. Organizácie by si mali uložené údaje chrániť pomocou šifrovania. Šifrovací kľúč by mala organizácia uchovávať interne.

Podniky majú tendenciu pozerať sa na rôzne zložky svojho podnikania z hľadiska celkových nákladov. Napríklad, ak majú spravovať svoj vlastný výpočtový systém, je potrebné na správu systému nielen udržiavať infraštruktúru, ale aj skúsených ľudí. Náklady na správu výpočtového systému teda presahujú náklady na infraštruktúru, a preto použitie cloudovej služby výrazne znižuje náklady. Organizácia navyše získavajú prístup k pokročilejším webovým službám, ako je online chat, online spracovanie kreditných

kariet a integrovaná webová stránka. Navyše je jednoduché získať nové zdroje a rýchlo ich implementovať. Napríklad spoločnosť, ktorá počas zdaňovacieho obdobia vyžaduje ďalší výpočtový výkon a úložný priestor, je schopná tieto služby získať na webe a uvoľniť ich, keď ich už nepotrebuje [B17, S14].

Výhody používania cloudu je možné zhrnúť ako:

- nižšie prevádzkové a servisné náklady pre používateľov, pričom platia len za to, čo používajú,
- škálovateľnosť/rozšíriteľnosť výpočtových kapacít na požiadanie, aby bolo možné splniť náročné a meniace sa požiadavky na výpočty,
- zdieľaný prístup k vzájomnej spolupráci, resp. tímovej práci podporujúcej zdieľané údaje/aplikácie,
- väčšia bezpečnosť údajov ako je schopná väčšina firiem poskytovať a spravovať vo svojich vlastných IT systémoch a priestoroch, predovšetkým z pohľadu zálohovania údajov,
- ľahká a rýchlejšia implementácia aplikácií,
- voľnosť používať veľké množstvo výpočtových zdrojov v cloude.

Obmedzenia pri zavádzaní cloudu do organizácie

Pred presunom do cloudu musia používatelia zvážiť niektoré obmedzenia spojené s cloud computingom a prípadne ich zahrnúť do zmluvy.

Zabezpečenie cloudu je najväčšou obavou používateľov cloudu. Táto obava pramení z viacerých dôvodov. Hlavným problémom mnohých používateľov je strata kontroly nad hardvérom a údajmi. Konštrukčne sa ku cloudovej infraštruktúre pristupuje prostredníctvom internetu. Zákazníci, ktorí sú zvyknutí mať prístup k vlastnej internej výpočtovej infraštruktúre, majú obavu, že keďže nevedia, kde je hardvér umiestnený, môže dôjsť k jeho ohrozeniu. Avšak poskytovatelia cloudových služieb majú vzhľadom na svoju veľkosť a technológie primerané zdroje na vybudovanie dostatočnej fyzickej bezpečnosti hardvéru, ako aj zabezpečenie záložných zdrojov elektrickej energie.

Druhým problémom je umiestnenie úložiska údajov v cloude. Poskytovateľ cloudových služieb je zodpovedný za ukladanie a zálohovanie údajov. Poskytovatelia služieb nasadzujú dostatok redundancie, aby zaručili vysoký stupeň dostupnosti služieb. Poskytovateľ služieb zvyčajne volí na umiestnenie redundancie lokality, ktoré sú od seba geograficky vzdialené, a to aj kvôli odolnosti voči prírodným katastrofám. Pre takto zabezpečené dáta je ťažké zákazníkovi určiť, kde sú jeho údaje uložené, hoci sú k dispozícii vždy, keď ich potrebuje. Niektoré krajiny vyžadujú, aby organizácie ukladali údaje o zákazníkoch v danej krajine. Je to z dôvodu rozdielnych právnych požiadaviek v jednotlivých krajinách týkajúcich sa ochrany súkromia. Krajiny Európskej únie majú výslovné zákony, ktoré vyžadujú, aby sa údaje ukladali v ich krajine/EÚ. Hlavným dôvodom je obava, že údaje uložené mimo regiónu, môžu byť zneužité cudzou vládou krajiny, v ktorej sú údaje uložené (USA, Čína, Rusko …).

Jedným z opatrení ako zabezpečiť dôvernosť údajov v cloude je šifrovanie uložených dát. Výhodou pre zákazníka je, ak si pred uložením dát do cloudu vyberie svoje vlastné šifrovanie. Zákazník by mal byť schopný si šifrovací kľúč zabezpečiť vo svojom vnútornom systéme.

Inou z obáv zákazníkov týkajúcou sa zabezpečenia cloudu je prenájom cloudových serveroch naraz viacerým zákazníkom. Poskytovatelia cloudových služieb ponúkajú zákazníkom virtuálne servery na rovnakom fyzickom servery a teda údaje patriace rôznym zákazníkom sa nachádzajú na tom istom fyzickom serveri a je obava, že k cudzím údajom by mohli mať prístup úmyselne alebo náhodne iní zákazníci. Hoci sú virtuálne servery oddelené, znepokojenie vyvoláva spôsob útoku založený na použití údajov, ktoré pretrvávajú v systémoch aj po ich použití, tzv. remanencia údajov. Potenciálni útočníci sa môžu napríklad prihlásiť na odber veľkého množstva úložného priestoru na virtuálnom serveri s úmyslom dostať sa k údajom, ktoré zostanú v úložnom priestore po použití iným zákazníkom. Tu dochádza k narušeniu dôvernosti klientov. Nebezpečenstvo umocňuje aj popularita modelu softvér ako služba (SaaS). S modelom SaaS môže viac klientov používať rovnaký softvér tretej strany a náhodne získať prístup k údajom iných klientov na rovnakom fyzickom serveri. Poskytovatelia cloudových služieb navyše vo svojich ponukách SaaS manipulujú s údajmi v otvorenej forme, t. j. nie zašifrovane. Navyše malé a stredné podniky, ktoré používajú cloudovú službu SaaS, nemajú finančné prostriedky, či odbornú znalosť zvládnuť zavedenie šifrovania svojich dát [S14].

Popularita cloudovej služby je založená na dostupnosti cloudu cez internet. Na používanie cloudovej služby nemusia zákazníci vlastniť žiadny špeciálny hardvér alebo softvér. Jednoduchosť prístupu cez internet však zvyšuje bezpečnostné obavy, pretože internet nie je navrhnutý ako bezpečná sieť. Zákazníci v cloude môžu túto nevýhodu prekonať pomocou služby VPN (Virtual Private Network) ponúkanej poskytovateľom telekomunikačných služieb. To však zvyšuje náklady na cloudové služby, a preto malé a stredné podniky zrejme VPN nevyužijú.

Dva ďalšie aspekty, ktoré sa tiež považujú za nedostatky pri vyžívaní cloud computingu, sa týkajú dôvery a kontroly dodržiavania bezpečnostných politík. Dôvera vyžaduje, aby poskytovateľ mal dobre definované politiky, ktoré sa riadia známymi normami. Napríklad poskytovateľ cloudových služieb by mal byť schopný poskytnúť zákazníkovi certifikácie tretích strán, s ktorými pri správe cloudu spolupracuje. Poskytovateľ služieb by mal byť schopný poskytnúť logovacie údaje zákazníkovi nejakým automatizovaným spôsobom, aby si zákazník bol vedomý svojich záväzkov a úrovne ich dodržiavania a mohol tak naplniť požiadavky poskytovateľa [S14].

Kľúčové obmedzenia cloudu sú [MB16]:

- je potrebný spoľahlivý a vždy dostupný vysokorýchlostný prístup k sieti/Internetu na pripojenie sa ku cloudu,
- je potrebné počítať s možnosťou občasnej pomalej reakcie cloudu a to z dôvodu zvýšenej premávky v sieti alebo vyššieho zaťaženia počítačov v cloude,

- riziko neoprávneného prístupu k údajom používateľov,
- strata údajov v dôsledku zlyhania cloudu (napriek replikácii na viacerých počítačoch),
- nie vždy stopercentná spoľahlivosť a nepretržitá dostupnosť služieb ponúkaných poskytovateľom cloudových služieb.

Zlyhania cloudových služieb

Napriek značným výhodám, ktoré cloud prináša, sa naďalej objavujú obavy z jeho používania. Ako už bolo uvedené, ide predovšetkým o otázky bezpečnosti a ochrany súkromia údajov a aplikácií v cloude. Uvedené dve oblasti predstavujú hlavné problémy používateľov pri prechode do cloudu. Na ne nadväzujú otázky spoľahlivosti a dostupnosti cloudových služieb, ako aj dodržiavanie záväzkov v cloudovom prostredí.

Uvedené obavy vyvolávajú aj niektoré predchádzajúce zlyhania cloudových služieb v minulosti. Príkladom je nepriame ovplyvnenie cloudovej infraštruktúry cez výpadok DNS serverov a preklad internetových domén spoločnosti Akamai v júni 2004. Potom, čo bol vykonaný útok na spoločnosť Akamai, nastal výpadok názvov domén, ktorý ovplyvnil chod stránok spoločnosti Google a Yahoo a mnoho ďalších webových stránok. Alebo v máji 2009 bola spoločnosť Google cieľom útoku odmietnutím služby (DoS), ktorý na niekoľko dní znesprístupnil služby Google News a Gmail.

Iným príkladom je výpadok služieb zapríčinený prírodnou katastrofou. V júni 2012 blesky spôsobili, že sa predĺžil čas odstávky spoločnosti Amazon, keďže AWS cloud vo východnej časti USA, ktorý pozostával z desiatich dátových centier v štyroch zónach dostupnosti, mal problémy s kolísaním energie. Búrka v danej lokalite znefunkčnila niektoré zariadenia spoločnosti Amazon a zasiahla spoločnosti využívajúce systémy výlučne v tomto regióne. Jednou z týchto obetí sa stala aj služba zdieľania fotografií Instagram. Zotavenie trvalo oveľa dlhšie ako sa predpokladalo a odhalilo celý rad problémov. Napríklad, jedno z desiatich centier nedokázalo prepnúť na záložné generátory pred tým, ako vyčerpalo energiu zo záložných zdrojov UPS. Zlyhalo aj prepínanie používateľov AWS na zdroje v inej oblasti. Proces zavádzania bol chybný a predĺžil sa čas na reštartovanie služieb EC2 a EBS. Ďalším kritickým problémom bola chyba v nástroji Elastic Load Balancer (ELB), ktorý sa používa na presmerovanie prenosov na servery s dostupnou kapacitou. Podobná chyba tiež ovplyvnila proces obnovy služby relačných databáz (RDS). Táto udalosť odhalila skryté problémy v infraštruktúre cloudu, ktoré sa však vyskytujú iba zriedka a aj to pri špecifických okolnostiach [M18].

Ďalšími rizikami stability cloudu sú chyby spôsobené interakčnými službami od rôznych poskytovateľov. Ak sa poskytovateľ cloudových aplikácií, poskytovateľ cloudových úložísk a sieťový poskytovateľ nedohodnú, môžu implementovať rôzne politiky. Takto vzniknuté nepredvídateľné interakcie medzi procesom vyrovnávania záťaže a inými mechanizmami môžu viesť k dynamickej nestabilite. Napríklad proces vyrovnávanie záťaže poskytovateľa aplikácie môže ovplyvňovať proces optimalizácie

energie poskytovateľa infraštruktúry. Niektoré z týchto iterácií sa môžu prejaviť iba v extrémnych podmienkach a pri normálnych prevádzkových podmienkach sa dajú veľmi ťažko zistiť, ale mohli by mať katastrofálne následky, keď sa systém pokúša zotaviť z ťažkej poruchy, ako to bolo v prípade poruchy v Amazone v 2012. Na druhej strane, umiestňovanie výpočtových a úložných zdrojov v rôznych dátových centrách v rôznych geografických lokalitách znižuje pravdepodobnosť katastrofických zlyhaní všetkých centier naraz. Toto geografické rozptýlenie zdrojov má ďalšie pozitívne vedľajšie účinky, ako je napríklad zníženie nákladov na energiu odoslaním výpočtov na miesta, kde je elektrická energia lacnejšia, alebo zlepšenie výkonu pomocou efektívnej stratégie vyrovnávania záťaže.

Niekedy má používateľ možnosť rozhodnúť sa, kde spustí aplikáciu, resp. vybrať si regióny, v ktorých sa budú inštancie jeho aplikácií spúšťať, ako aj regióny úložísk. Takéto rozhodnutie však sťažuje optimalizáciu celého systému. Ciele systému, čo je maximálna priepustnosť, využitie zdrojov a finančné výhody, musia byť starostlivo vyvážené potrebami používateľov, a to nízkymi nákladmi, malým časom odozvy a maximálnou dostupnosťou. Avšak akákoľvek optimalizáciu v systéme je zaplatená zvýšenou zložitosťou daného systému. Napríklad oneskorenie komunikácie cez WAN sieť/internet je značne väčšia ako latencia v sieti LAN a vyžaduje si vývoj nových algoritmov pre globálne rozhodovanie [M18].

Na lepšie zabezpečenie požadovanej úrovne poskytovania služieb a obmedzenie záväzkov sa pri využívaní cloudových služieb dôrazne odporúča organizácii uzavrieť dohodu o úrovni poskytovaných služieb (SLA, service-level agreement) s poskytovateľom cloudu. SLA špecifikuje podmienky, ako aj očakávania používateľa a povinnosti poskytovateľa cloudových služieb, čo, kedy a do akých termínov musí dodržať a zabezpečiť. Starostlivým plánovaním a začlenením požiadaviek používateľa do ponúk cloudových služieb môžu poskytovatelia cloudu, ako aj používatelia, znížiť možné riziko a ťažiť z výhod hosťovaných služieb založených na cloude.

Výber cloudu

S prechodom na cloudové technológie musí organizácia zmeniť aj celkovú koncepciu svojho chodu. Aby organizácia úspešne využívala výhody cloudu, musí sa na prechod pripraviť strategicky, kultúrne a organizačne a musí mať ucelený pohľad na cloud computing. Organizácia si zvolí pre ňu najvhodnejšiu cloudovú alternatívu z dostupných cloudov, zváži si a riadi riziká spojené s migráciou dát a služieb na cloud pomocou bezpečnostných opatrení. Prechod do cloudu nie je však len o technológii, proces migrácie do cloudu by mal zo sebou niesť aj zmeny v pracovnej náplni zamestnancov, firemných procesov a služieb, ako aj procesoch riadenia zmien. Prechod na cloud vyžaduje tiež nový druh IT manažmentu a riadiaceho rámca.

Hlavné rozhodnutie, ktoré musí IT manažment organizácie urobiť, je typ cloudu, či bude v organizácii využívaný verejný alebo privátny cloud alebo ich variácie, a či to bude zodpovedať požadovaným aplikáciám z cloudu. IT manažment musí poznať rozdiely

jednotlivých modelov cloudov, ako aj riziká, ktoré sú s nimi spojené a to aj v súvislosti s charakteristikami a požiadavkami ich aplikácií. IT manažment musí tiež zvážiť [MB16]:

- výkonnostné požiadavky, bezpečnostné požiadavky, dostupnosť a kontinuitu cloudových služieb,
- množstvo prenášaných dát medzi používateľmi a cloudom a/alebo medzi rôznymi cloudami,
- citlivú povahu aplikácií,
- kontrolu aplikácií a údajov,
- celkové súvisiace náklady,
- či sú externí poskytovatelia cloudu dôveryhodní,
- podmienky, ktoré vyžadujú externí poskytovatelia cloudu,
- interné technické schopnosti.

Virtualizácia

Virtualizácia sa využívaná od šesťdesiatych rokov minulého storočia v oblasti výpočtovej techniky a pre cloud predstavuje jeden zo základných pilierov. Ide o všeobecný pojem, ktorý sa vzťahuje na abstrakciu výpočtových zdrojov. Vo všeobecnosti ide o techniku na skrývanie fyzických charakteristík výpočtových zdrojov (CPU, pamäť, disk a sieťové rozhrania) pred spôsobom, akým iné systémy, aplikácie alebo koncoví používatelia interagujú s týmito zdrojmi. Virtualizácia vytvára externé rozhranie, ktoré skryje základnú implementáciu pomocou kombinácie zdrojov na rôznych fyzických miestach alebo zjednodušením riadiaceho systému [MB16].

Ďalším kľúčovým konceptom je *zapuzdrenie*, čo znamená, že všetky súbory spojené s virtualizovaným operačným systémom (OS), aplikáciou a podporným softvérom sa ukladajú ako jeden veľký súbor alebo virtuálny disk. Prostredníctvom zapuzdrenia sa môže stav virtuálneho počítača uložiť na disk a potom sa môže virtuálny stroj reštartovať na opätovné načítanie údajov z disku. Nedávny vývoj nových virtualizačných platforiem pre VMware, Citrix a ďalšie, zameral pozornosť práve na tento koncept. Virtualizačný softvér, akým je vSphere od VMware, XEN od Citrix a Hyper-V od spoločnosti Microsoft, dokáže transformovať alebo virtualizovať hardvérové zdroje počítača s procesorom x86, vrátane CPU, RAM, pevného disku a sieťového radiča, a tak vytvoriť plne funkčný virtuálny stroj, ktorý prevádzkuje svoj vlastný operačný systém a aplikácie rovnako ako „skutočný“ počítač. Virtuálne počítače môžu pokrývať väčšinu operačných systémov x86 (napr. Windows, Linux alebo Solaris x86). Viaceré virtuálne stroje zdieľajú hardvérové zdroje jedného fyzického počítača bez vzájomného rušenia sa, takže jeden počítač môže súčasne spúšťať niekoľko operačných systémov a aplikácií, bežne označovaných ako pracovné zaťaženie.

Virtualizácia sa vo všeobecnosti uskutočňuje umiestnením tenkej vrstvy softvéru priamo na hardvér počítača alebo na hostiteľský operačný systém. Táto softvérová vrstva obsahuje hypervízor (monitor) virtuálneho počítača, ktorý dynamicky a transparentne alokuje hardvérové prostriedky tak, aby viacero operačných systémov, z ktorých každý

je obsiahnutý vo vlastnom virtuálnom stroji, bolo spustených súčasne na jednom fyzickom počítači. Hypervízor je pre hosťovaný systém najvyšším arbitrom, ktorý riadi prístup virtualizovaných počítačov k hardvéru hostiteľského počítača, riadi ich beh a zároveň ich od seba oddeľuje. V prípade VMware sa hypervízor označuje ako server ESXi. Je dôležité pochopiť, že virtuálny stroj môže byť takmer akýmkoľvek operačným systémom x86 s pridruženými aplikáciami. Napríklad fyzický hostiteľ Microsoft Hyper-V môže prevádzkovať tri samostatné virtuálne stroje; prvým virtuálnym strojom by mohol byť operačný systém Solaris X86 a databáza, druhým virtuálnym strojom by mohol byť Windows Server 2012 a MS Exchange a tretím operačným systémom Linux s balíkom softvéru LAMP pre implementáciu dynamických webových stránok, ktorý používajú vývojári [GJ18, MB16].

Existuje niekoľko presvedčivých argumentov, ktoré vedú organizácie k zavádzaniu virtualizácie vo svojich dátových centrách. Virtualizácia je praktický spôsob, ako optimalizovať dátové centrá, znížiť náklady, ako aj spotrebu energie. Väčšina nevirtualizovaných serverov pracuje s 5 – 15 % kapacity, čo je vysoko neefektívne. Pretože organizácie väčšinou vlastnia oveľa viac fyzických serverov, ako je potrebné, dnešné dátové centrá sú niekoľkokrát väčšie a zodpovedajúcim spôsobom neefektívne. Pri virtualizácii serverov je bežná prevádzková efektívnosť 70 – 75 %, niekedy aj vyššia. Na druhej strane, takto vyťažené servery spotrebujú aj viac energie na svoje fungovanie a chladenie [MB16]. Preto je pri zavádzaní virtualizácie potrebné zvážiť, či sa oplatí, a to jednak z finančného pohľadu, ale aj z potreby zamestnať špecialistov, ktorí majú skúsenosti s danou technológiou.

Existujú tri základné typy virtualizácie, a to *hardvérová virtualizácia*, *virtualizácia úložného priestoru* a *virtualizácia siete*.

Pri pojme virtualizácia sa dnes zvyčajne prioritne berie *hardvérová virtualizácia*. Virtualizácia hardvéru je zdieľanie fyzických systémových prostriedkov (CPU, pamäte, siete a lokálneho úložiská), ktoré umožňuje spustenie viacerých virtuálnych počítačov na rovnakom fyzickom serveri. Existujú tri hlavné typy virtualizácie hardvéru alebo servera, a to úplná virtualizácia, paravirtualizácia a hardvérovo podporovaná virtualizácia, Obrázok 0-6. V posledných rokoch sa k nim pridáva aj kontajnerová virtualizácia.

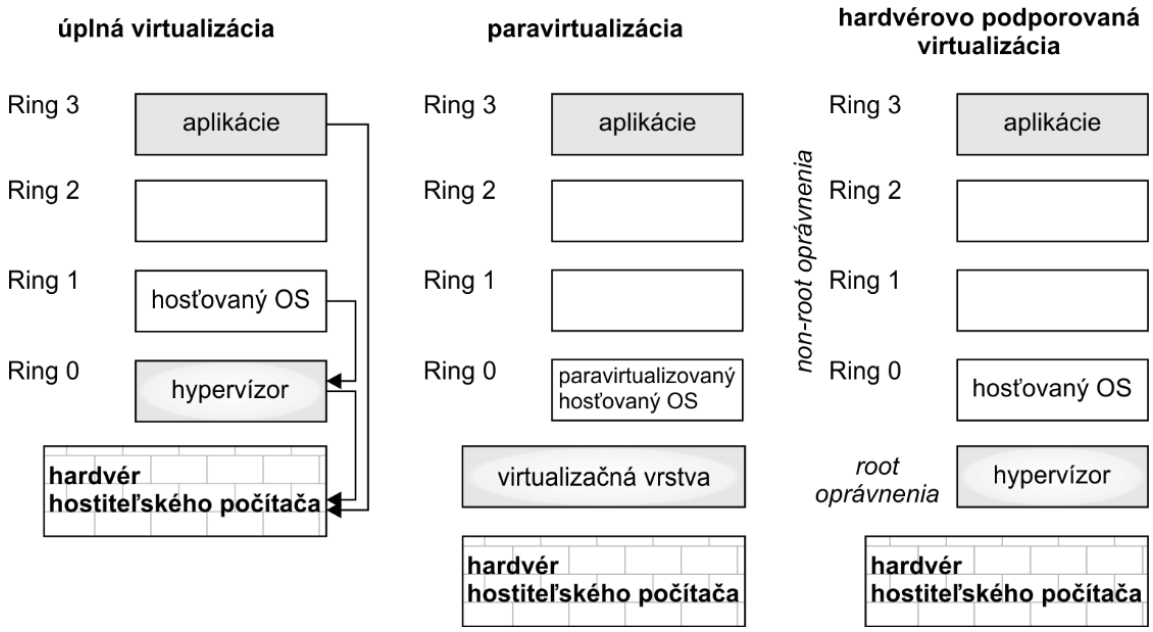
Úplná virtualizácia patrí medzi najstaršie typy virtualizácie, kde sa pre každý hosťovaný systém vytvára rovnaká kópia fyzickej architektúry, čo umožňuje virtuálnemu stroju pozostávajúcemu z operačného systému a aplikácií fungovať bez zmeny. Dnešní moderní poskytovatelia virtualizácie môžu virtualizovať akýkoľvek operačný systém x86 kombináciou techník binárneho prekladu a priameho vykonávania. Binárny preklad prekladá kód jadra, aby nahradil nevirtualizovateľné inštrukcie novými sekvenciami inštrukcií, ktoré majú požadovaný účinok na virtuálny hardvér. Medzitým sa na hostiteľskom procesore vykoná čo najviac žiadostí o procesor, aby sa dosiahol vyšší výkon. Týmto spôsobom má každý virtuálny stroj všetky služby fyzického systému, vrátane virtuálneho systému BIOS, virtuálnych zariadení a správy virtualizovanej pamäte. Kombinácia binárneho prekladu a priameho vykonávania poskytuje úplnú

virtualizáciu, pretože hosťujúci OS je virtualizačnou vrstvou úplne abstrahovaný (úplne oddelený) od základného hardvéru. Hosťujúci OS si nie je vedomý toho, že je virtualizovaný, a preto nevyžaduje žiadne úpravy.

Pri *paravirtualizácii* je snaha dosiahnuť vyššiu rýchlosť za cenu pridania priamej komunikácie medzi operačným systémom virtuálneho stroja (VM) a hostiteľským operačným systémom. Virtuálny stroj nie je plne hardvérovo emulovaný, ale je vytvorené akési programové rozhranie pre využitie skutočného hardvéru. Paravirtualizácia sa využíva predovšetkým vtedy, ak sa niektoré komponenty virtuálneho stroja zhodujú s fyzickým počítačom. Aby to bolo možné, je potrebný operačný systém s upraveným jadrom.

Kontajnerová virtualizácia alebo virtualizácia na úrovni operačného systému je ďalší z možných implementácii celého riešenia. Virtualizácia na úrovni operačného systému využíva pre svoj beh jadro operačného systému hostiteľského počítača. Ide o odľahčenú virtualizáciu, ktorá nesimuluje celý hardvér, nad ktorým beží virtuálny počítač. Virtuálne počítače, tzv. kontajnery, zdieľajú jadro operačného systému hostiteľa. Aktuálne najznámejšia kontajnerová virtualizácia je Docker. Docker na izoláciu kontajnerov využíva Linuxové technológie ako namespace (oddelenie sieťovej komunikácie) a cgroups (control groups – funkcia linuxového jadra na limity a izoláciu systémových zdrojov pre jednotlivé procesy a skupiny procesov). Umožňuje napríklad hladko presúvať aplikácie a služby medzi hostiteľskými servermi, obsahuje nástroje pre správu bitových kópií. Napríklad je možné vytvoriť kontajner typu Docker, ktorý nerobí nič iné, než že v ňom funguje služba memcached pre Apache Web server. Tento kontajner sa môže urobiť zo štandardného Linuxu, ako sú Ubuntu alebo CentOS, a požadovaná služba sa nainštaluje a nakonfiguruje rovnako ako na akomkoľvek Linuxe. Kontajner možno potom odovzdať do riadenia verzií Git a prevádzkovať na ľubovoľnom ďalšom systéme, kde ho je možné okamžite spustiť a stane sa z neho vlastne funkčná produkčná služba. Tak je možné inštanciu memcached replikovať a spúšťať na virtuálnom serveri, fyzickom serveri, v cloude Amazon alebo kdekoľvek inde, kde je možné Docker spustiť. Nie je potrebné sa starať o závislosti služieb medzi hostiteľmi, ani o inštaláciu aplikácií, emuláciu hardvéru či čokoľvek zo zložitosťou tradičnej virtualizácie. Stačí len spustiť správne vytvorený kontajner tam, kde je ho treba prevádzkovať.

Hardvérovo podporovaná virtualizácia je rozšírená najmä v dátových centrách, kde virtualizovaný operačný systém je nad vrstvou softvérovej platformy a beží priamo na hardvéri bez operačného systému. Umožňuje spúšťanie jednotlivých virtualizovaných operačných systémov priamo nad jedným hardvérom bez nutnosti existujúceho operačného systému. Výhodou tejto virtualizácie je úplné využitie hardvérových prostriedkov pre virtualizované operačné systémy.



Obrázok 0-6 Typy virtualizácie

Okrem hardvérovej virtualizácie existujú aj ďalšie typy virtualizácie, ktoré sa používajú v cloud computingu, a to virtualizácia úložného priestoru a virtualizácia siete.

Virtualizácia úložného priestoru sa vo všeobecnosti vzťahuje na abstrakciu fyzických zdrojov úložného priestoru (disky, pamäť, radiče atď.). Virtualizácia úložného priestoru znamená, že všetky platformy úložného priestoru sú virtualizovaným serverom prezentované jednotným spôsobom. To znamená, že je možné vidieť a spravovať dáta ako jeden logický prostriedok bez ohľadu na to, kde sa fyzicky nachádzajú v typickej rôznorodej skupine úložných systémov a sietí. Výhodou je, že správca diskov môže presúvať bloky údajov tak, aby získal efektívnosť ukladania bez toho, aby používateľ videl nejaké zmeny. Navyše, úložné zariadenia od rôznych výrobcov možno spravovať, akoby išlo o jednu heterogénnu úložnú platformu. Je možné migrovať dáta (a virtuálne stroje) medzi úložnými platformami. Toto je jedna z hlavných výhod, ktoré virtualizácia poskytuje, a je to jedna z mnohých funkcií, vďaka ktorým je virtualizácia základným pilierom cloud computingu.

Virtualizácia siete predstavuje logické sieťové zariadenia a služby, t. j. logické porty, prepínače, smerovače, firewall, vyrovnávače zaťaženia, VPN a ďalšie, bez ohľadu na základný fyzický hardvér. Problémom bežných sieťových a bezpečnostných riešení je ich nedostatočná prispôsobivosť, zložitosť a nekompatibilita s riešením iných výrobcov. To všetko dohromady bráni podnikom naplno využívať výhody modelu softvérovo definovaného dátového centra, predovšetkým čo sa týka pružnosti, efektivity a optimalizácie nákladov. Vďaka virtualizácii sietí môžu prevádzkovatelia dátových centier zaobchádzať s fyzickými sieťami ako so zdrojom transportnej kapacity, ktorý možno využívať a meniť podľa požiadaviek. Vo všetkých ostatných ohľadoch virtuálne

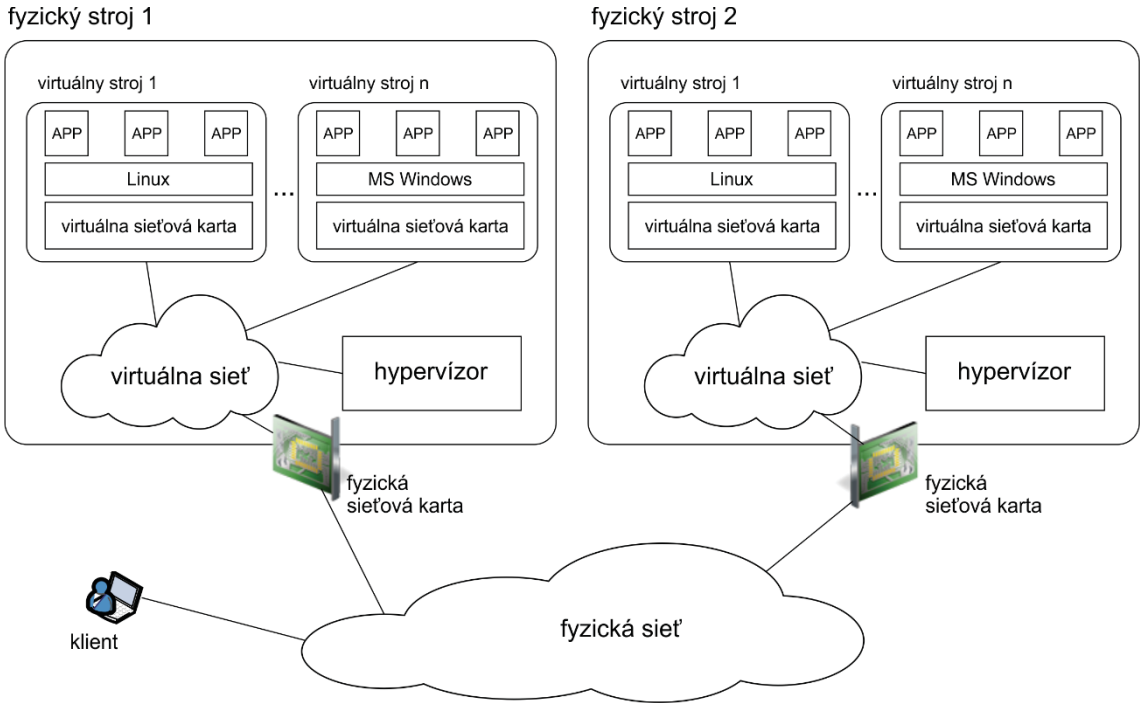
stroje bežia vo virtuálnej sieti presne tak, ako keby bežali vo fyzickej sieti. Virtuálna sieť je v podstate sieť vytvorená nad fyzickou sieťou.

Virtualizácia externej siete kombinuje alebo rozdeľuje jednu alebo viac lokálnych sietí (LAN) na virtuálne siete, aby sa zvýšila účinnosť veľkej siete alebo dátového centra. Kľúčové komponenty tvorí virtuálna lokálna sieť (VLAN) a sieťový prepínač. Pomocou tejto technológie môže správca systému nakonfigurovať systémy fyzicky pripojené k tej istej lokálnej sieti do samostatných virtuálnych sietí. Naopak, správca môže kombinovať systémy v samostatných lokálnych sieťach (LAN) do jedného segmentu VLAN, ktorý pokrýva veľkú sieť.

Virtualizácia vnútornej siete konfiguruje jediný systém pomocou softvérových kontajnerov, ako sú programy na riadenie hypervisora Xen, alebo pseudo-rozhrania, ako napríklad VNIC, na emuláciu fyzickej siete so softvérom. To môže zlepšiť efektívnosť jedného systému izoláciou aplikácií na oddelenie kontajnerov alebo pseudo-rozhraní [MB16].

Virtualizovaná sieť má rovnaké vlastnosti ako fyzická sieť, ale prináša prevádzkové výhody a nezávislosť hardvéru. Všetky atribúty fyzickej siete sú logicky mapované a prezentované virtuálnym strojom. Virtualizovaná sieť umožňuje automatizovanú údržbu, pretože premapovanie fyzických na logické zariadenia môže nastať bez prerušenia chodu systému. Následne môže prebiehať údržba fyzických zdrojov, môžu byť nahradené alebo inovované a mapovanie sa môže obnoviť bez prerušenia pracovnej záťaže. Všetky virtualizačné technológie, server, úložisko a sieťové pripojenie tak môžu byť zahrnuté v tzv. softvérovom dátovom centre (SDDC, Software-defined Datacenter) a poskytované ako služba [BEE16].

Obrázok 0-7 znázorňuje vytvorenie virtuálnych sietí nad fyzickou sieťou. Na obrázku je znázornená LAN pozostávajúca z klienta, niekoľkých fyzických spojení a dvoch ďalších fyzických počítačov. Rovnako ako v prípade virtuálnych strojov je používaný hypervízor. V tomto prípade hypervízor vytvorí virtuálnu sieťovú kartu (vNIC, virtual Network Interface Card) pre každý virtuálny stroj. Každý fyzický stroj sám prevádzkuje virtuálnu sieť, virtuálne sieťové karty a hypervízor. Virtuálne sieťové karty vNIC sú v tomto prípade používané virtuálnymi strojmi. Komunikácia medzi virtuálnymi strojmi vo fyzickom stroji prebieha cez miestnu virtuálnu sieť. Virtuálne stroje jedného fyzického stroja môžu navzájom komunikovať prostredníctvom príslušnej virtuálnej siete. Keďže sa však virtuálna sieť pripája aj k fyzickej sieťovej karte a teda k fyzickej sieti, ktorýkoľvek z virtuálnych strojov môže komunikovať aj s externými zariadeniami vrátane virtuálneho stroja iného fyzického počítača [FH17].



Obrázok 0-7 Sieťová virtualizácia.

Okrem schopnosti virtualizácie migrovať pracovné zaťaženie na rôzne platformy a miesta, čím sa šetria finančné náklady organizácie, je ďalším dôležitým prínosom nasadenia virtualizácie do IT infraštruktúry organizácie schopnosť virtualizácie uľahčiť proces zotavenia systému do pôvodného stavu.

Zotavenie systému po havárii je proces, ktorým organizácia obnoví svoju činnosť do pôvodného stavu, v akom bol pred haváriou. Pod haváriou si je možné predstaviť udalosť veľkých rozmerov, ako je prírodná katastrofa (napríklad zemetrasenie alebo požiar) alebo teroristické útoky, ale haváriou môže byť aj udalosť menších rozmerov ako napríklad poruchy softvéru spôsobené počítačovými vírusmi alebo výpadok elektrického napájania v dátovom centre. Práve virtualizácia napomáha spoločnosti s procesom zotavenia po takejto udalosti a to vďaka konceptu zapuzdrenia. Ako už bolo spomenuté vyššie, vo virtuálnom prostredí sú OS, aplikácie a všetko na fyzickom pevnom disku fyzického servera zapuzdrené ako jeden veľký súbor. Vďaka zapuzdreniu sú virtuálne stroje spolu s úlohami na nich vykonávanými iba veľké súbory a existuje pri ich manipulácii značná flexibilita.

Virtuálne stroje sa môžu napríklad kopírovať a zálohovať v inej lokalite, t. j. v inom dátovom centre ako je virtualizovaný priestor realizovaný virtualizovaným serverom. Navyše zálohovací priestor nemusí byť nevyhnutne od toho istého výrobcu ako pôvodný virtualizačný priestor. Virtualizácia tak do istej miery normalizuje základné fyzické prostriedky servera a virtualizované prostredie je možné bez problémov kopírovať z jednej značky servera na inú. Spoločnosť VMware má dokonca produkt zvaný Site Recovery Manager (SRM), ktorý má pomôcť pri procese zotavenia tak, že pomáha dokumentovať a vylepšovať plán obnovy po havárii. Proces zotavenia nie je taký

triviálny. Napríklad, ak je primárne dátové centrum z dôvodu prírodnej katastrofy vymazané a našťastie prebehlo vytvorenie zálohy všetkých potrebných častí systému do sekundárneho dátového centra, vyvstáva otázka, ktoré úlohy sú pri zotavení prioritné a v akom poradí. Služba e-mail je zrejme jedna z prvých v zozname priorít. Ale sú tu pravdepodobne veci, ktoré sa musia obnoviť ešte skôr, napríklad DNS alebo Active Directory alebo množstvo ďalších činností, na ktoré by sa zrejme v prípade časového stresu zabudlo. Produkt Site Recovery Manager umožňuje správcom otestovať ich plán zotavenia a automatizuje proces testovania bez nutnosti narušenia bežnej prevádzky organizácie. Virtualizačné technológie preukázali, že zotavenie po havárii bolo jednoduchšie, spoľahlivejšie a rýchlejšie práve s využívaním virtualizovaného prostredia [GJ18, MB16].

Manažment cloudu

Cloud nie je len jedna technológia, ide o komplexný systém s veľmi veľkým počtom zdieľaných zdrojov, ktoré podliehajú nepredvídateľným požiadavkám a sú ovplyvnené externými udalosťami, ktoré nie je môže mať vždy pod kontrolou. Manažment cloudových prostriedkov vyžaduje zložité politiky a rozhodnutia pre celkovú optimalizáciu. Správa cloudových prostriedkov je mimoriadne náročná z dôvodu zložitosti systému, ktorý znemožňuje mať presné informácie o globálnom stave a z dôvodu nepredvídateľnej interakcie s prostredím.

Stratégie riadenia zdrojov spojené s tromi základnými modelmi poskytovania cloudu, IaaS, PaaS a SaaS, sú rôzne. Vo všetkých prípadoch čelia poskytovatelia cloudových služieb veľkým kolísavým zaťaženiam. Pri niektorých udalostiach je možné už vopred predpokladať nárast na požiadavky na cloudové zdroje, a tak môžu byť zdroje vopred vyhradené. Napríklad je to pri niektorých webových službách, ktoré sú predmetom sezónnych špičiek (voľby, Vianoce, Black Friday …). Medzi základné politiky manažmentu cloudu patria [MB16]:

- energetická optimalizácia,
- kontrola vstupov,
- prideľovanie kapacity,
- vyrovnávanie záťaže,
- kvalita služieb (QoS).

Úlohou kontroly vstupov je zabrániť systému v tom, aby prijal ďalšie pracovné zaťaženie v rozpore s politikou systému. Napríklad systém nemusí akceptovať ďalšie úlohy, ktoré by mu bránilo dokončiť už prebiehajúce práce alebo ohrozili splnenie termínu vykonania zadaných úloh. Takéto obmedzenia si však vyžadujú mať znalosti globálneho stavu celého systému. Ako sa zväčšuje samotný systém, je čoraz náročnejšie udržiavať si prehľad o jeho celom stave. Navyše, v dynamickom systéme sa jeho stav neustále mení a je potrebné informácie aktualizovať.

Politika prideľovania kapacity sa zaoberá prideľovaním jednotlivých zdrojov v cloude pre konkrétne prípady, t. j. pri aktivácii služby. Lokalizácia zdrojov, na ktoré sa vzťahujú

viaceré globálne obmedzenia kvôli ich optimalizácii, si vyžaduje rýchle vyhľadávanie vo veľkom priestore, navyše za predpokladu, že sa stav jednotlivých podsystémov mení rýchlo. Vyrovnávanie záťaže a optimalizácia energie sa môžu vykonávať na miestnej úrovni, ale globálne politiky vyrovnávania záťaže a optimalizácie energie čelia obdobným problémom. Navyše, vyrovnávanie záťaže a optimalizácia energie sú vo vzájomnej korelácii a ovplyvňujú náklady na poskytovanie služieb. Medzi základnými politikami, ako aj mechanizmami ich vykonávania sú silné vzájomné závislosti. Mnoho mechanizmov na manažovanie cloudu sa sústreďuje na výkonnosť systému z hľadiska priepustnosti a optimalizácie času, ale zriedka zahŕňajú aj optimalizáciu energie alebo záruky dodržiavania kvality služieb [OAF18].

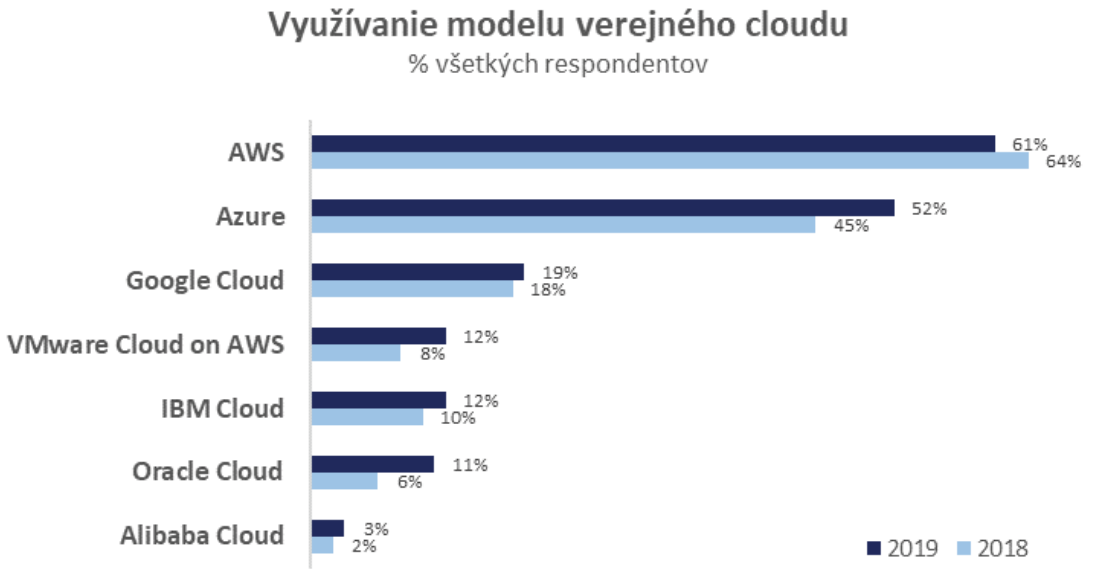
Poskytovatelia cloudových služieb majú spravidla svoje vlastné riešenia na manažovanie cloudu, prostredníctvom ktorých spravujú svoj cloud z dátových centier. Mnohé špecializované spoločnosti, ktoré sa v minulosti podieľali na vývoji produktov na správu siete, sa v súčasnosti zameriavajú na zabezpečenie a správu cloudového prostredia a ponúkajú svoje produkty poskytovateľom cloudových služieb. Následne poskytovatelia cloudu spolu s týmito spoločnosťami ponúkajú zákazníkom širokú škálu riešení správy cloudu. Každé z týchto riešení sa zameriava na inú množinu cloudových funkcií a má svoju jedinečnú prednosť. Napríklad VMware vRealize Business je nástroj na využitie zdrojov a sledovanie nákladov. Aplikácia Dell Cloud Manager pomáha zvyšovať pružnosť a správu v cloude. Neexistuje teda jediné najlepšie riešenie, ktoré by poskytovatelia cloudov mohli použiť na správu svojich cloudov. Výber najvhodnejšieho nástroja na správu cloudu by mal skôr závisieť od požiadaviek podnikania.

Na trhu existuje aj niekoľko neutrálnych riešení/platforiem na manažovanie cloudu. Dell Cloud Manager je jedno z riešení, ktoré je ponúkané ako SaaS na manažovanie cloudovej infraštruktúry vrátane poskytovania a správy aplikácií a možno ho tiež nasadiť lokálne ako softvér na riadenie všetkých typov cloudových modelov. Môže pracovať s viacerými verejnými cloudmi vrátane AWS, VMware a Microsoft Azure a dokonca môže spravovať prostredie opensource, ako je OpenStack. Ďalší nástroj vRealize Business od spoločnosti VMware je možné použiť s rôznymi verejnými, privátnymi a hybridnými cloudmi. Cloudyn je zas riešenie, ktoré je prispôsobené pre nasadenie AWS, Microsoft Azure, Google a OpenStack. Ďalšie významné riešenia v oblasti správy cloudov ponúka spoločnosť BMC Software, CA Technologies, IBM, HP, Red Hat a iné [B17].

Poskytovatelia cloudov

Ako už bolo zmienené vyššie, základnými modelmi služieb cloudu sú softvér ako služba (SaaS), platforma ako služba (PaaS) a infraštruktúra ako služba (IaaS). Najbežnejšie modely nasadenia cloudu sú verejný cloud, privátny, komunitný a hybridný cloud. Hlavnými poskytovateľmi cloudových služieb, ktorí sú aj bližšie rozoberaní v tejto podkapitole, sú spoločnosti Amazon Web Services (AWS), Google Apps, Microsoft Azure a Office 365, IBM Cloud, Oracle Cloud, Alibaba Cloud, Dropbox, Apple iCloud

a VMware Cloud on AWS. Obrázok 0-8 znázorňuje postavenie najväčších hráčov na trhu v oblasti verejného cloudu.



Obrázok 0-8 Využívanie modelu verejného cloudu používateľmi podľa veľkosti poskytovateľov [R19].

Amazon Web Services (AWS)[9] je najväčší poskytovateľ cloudových služieb na svete a ponúka služby ako Elastic Compute Cloud (EC2) a Simple Storage Service (S3). Jeho trhová kapitalizácia je taká, že počítačové zdroje využívané rôznymi podnikmi prostredníctvom Amazonu sú päťkrát väčšie ako všetky ostatné cloudové služby dohromady. AWS ponúka aj bezplatnú testovaciu úroveň použitia podobnú e-mailovým službám od spoločnosti Google, Yahoo a Microsoft.

AWS poskytuje zákazníkom jediné kontaktné miesto pre všetky cloudové služby. To je užitočné najmä vtedy, keď sa zákazník prispôsobuje cloudovému prostrediu. Spoločnosť Amazon uviedla AWS na trh v roku 2006. Túto infraštruktúru v priebehu rokov neustále rozširovala. Celková investícia spoločnosti Amazon do cloudovej infraštruktúry je približne 12 miliárd dolárov, čo je menej ako v prípade iných hlavných poskytovateľov cloudových služieb. Napriek nižším investíciám je spoločnosť AWS schopná ponúkať svoje cloudové služby na celom svete. Má niekoľko tisíc zákazníkov v 190 krajinách.

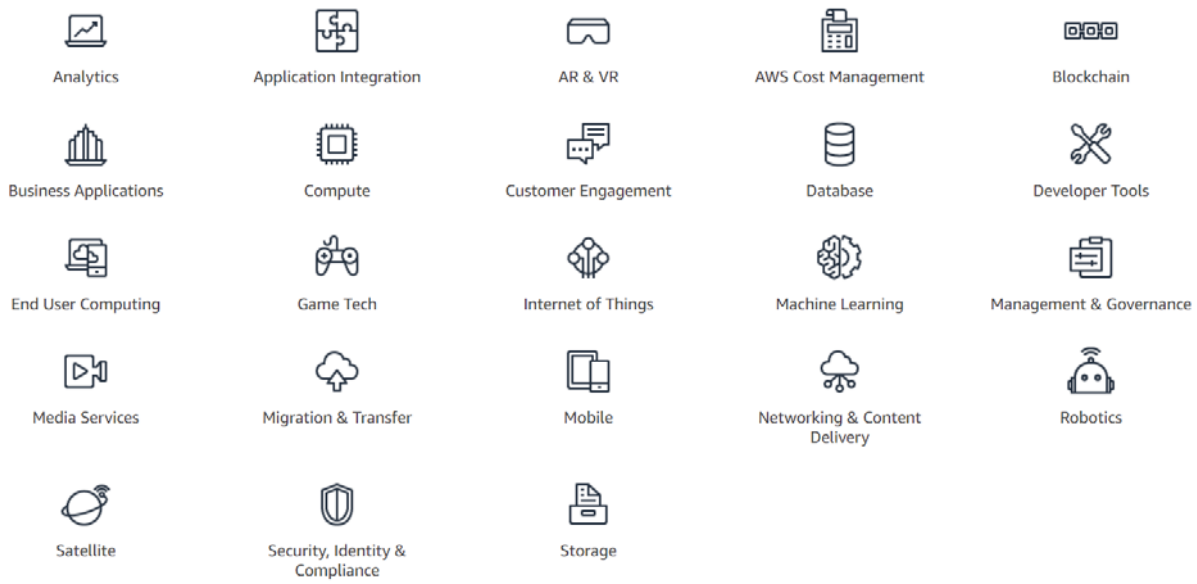
AWS ponúka služby SaaS, PaaS a IaaS a tiež využíva modely verejného a privátneho cloudového nasadenia. Služby AWS využívajú spoločnosti všetkých veľkostí. Napríklad Dropbox, ktorý bol priekopníkom v ukladaní a zdieľaní súborov v cloude, využíva službu AWS S3 na ukladanie všetkých súborov svojich zákazníkov, čo sa počíta na niekoľkých miliárd súborov. Pružnosť dopytu, ktorú poskytuje služba S3, umožňuje Dropboxu využívať toľko miesta, koľko je potrebné na uloženie všetkých súborov zákazníkov,

[9] https://aws.amazon.com/

s intenzitou až 1 miliarda súborov za deň. Dropbox tiež používa svoje vlastné servery, ale nepoužíva ich na ukladanie súborov zákazníkov. Okrem Dropboxu patria medzi významné veľké spoločnosti využívajúce cloudové služby AWS Netflix, Flickr a Pinterest.

Vzhľadom na veľkú popularitu AWS je množstvo zákazníkov na celom svete závislých od dostupnosti AWS vo všetkých časových pásmach. Takže aj malý výpadok služieb v spoločnosti AWS má veľký vplyv na poskytovanie rôznych služieb po celom svete. Uvedenú skutočnosť prakticky potvrdilo niekoľko významných výpadkov AWS za posledné roky. Niektoré z týchto výpadkov boli spôsobené prerušením napájania AWS, zatiaľ čo iné boli spôsobené ľudskou chybou. AWS zväčša po výpadku prichádza s podrobnou analýzou príčin výpadku a sprístupňuje svoje zistenia zákazníkom [S14].

V roku 2019 spoločnosť AWS ponúkala viac ako 165 služieb zahŕňajúcich širokú škálu služieb vrátane výpočtovej techniky, ukladacieho priestoru, sietí, databáz, analytických služieb, aplikačných služieb, nasadenia softvéru, manažmentu, mobilných, vývojových nástrojov a nástrojov pre internet vecí, Obrázok 0-9 znázorňuje rozmanitosť ponúkaných produktov. Väčšina služieb nie je priamo sprístupnená koncovým používateľom, ale namiesto toho ponúka vývojárom prostredníctvom rozhrania API rôznu funkcionalitu na použitie v ich aplikáciách. Ponuky služieb Amazon Web Services sú prístupné prostredníctvom protokolu HTTP pomocou architektonického štýlu REST a protokolu SOAP. AWS má aj isté nevýhody. Medzi nevýhody patrí pomerne vysoká cena pre vytvorenie vlastného riešenia, ktoré obsahuje špecifické požiadavky. Rovnako je nevýhodou problém s kompatibilitou databáz, Amazon Aurora, Redshift a DynamoDB sú kompatibilné iba s AWS. V neposlednom rade je to aj nedostatočná spolupráca s komunitami s otvoreným zdrojom.



Obrázok 0-9 Ponuka všetkých produktov Amazon Web Services[10].

[10] https://aws.amazon.com/products/

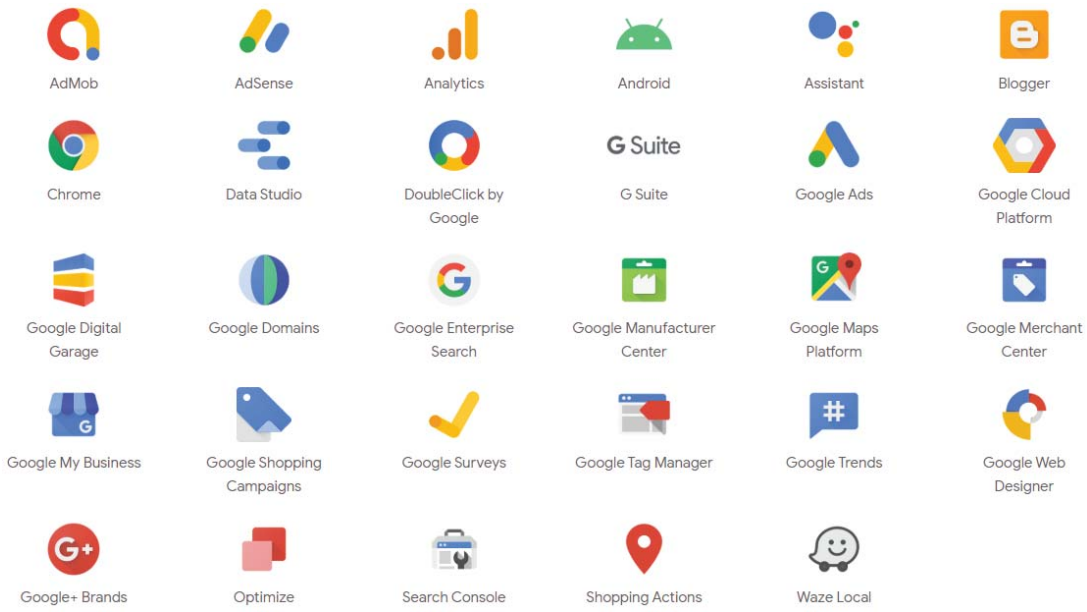
Google Apps[11] – aplikácie spoločnosti Google zaznamenali v poslednej dobe značný rozmach. Pôvodnou aplikáciou boli Dokumenty Google, ktoré boli uvedené na trh v roku 2006. Aplikácia Dokumenty Google bola navrhnutá tak, aby poskytovala možnosť vytvárania a zdieľania dokumentov a tabuliek na webe. Výhodou, s ktorou služba Dokumenty Google prišla, bolo poskytnutie zákazníkovi aplikáciu, ktorá umožňuje zdieľanie súborov v rôznych formátoch, nahrávanie alebo sťahovanie súborov v rôznych formátoch, priame publikovanie súborov vo formáte HTML, ako aj udržiavanie súborov na požiadanie iba v jednom formáte. Pôvodnou cloudovou službou spoločnosti Google bola služba Gmail. Službu Gmail v máji 2018 používalo celosvetovo viac ako 1,5 miliardy aktívnych používateľov.

Spoločnosť Google rozšírila svoje aplikácie Google na Gmail, Dokumenty Google, Disk Google, Google Talk, Kalendár Google, YouTube, Google Labs a Google Play. Všetky tieto služby sú medzi verejnosťou veľmi obľúbené, pretože sú pre verejnosť bezplatné. Disk Google má napríklad kapacitu 15 GB a služba Google Talk umožňuje zákazníkom bezplatne komunikovať prostredníctvom webu v hovorenom formáte. Najnovšia aplikácia, Google Play, je komplexná služba, ktorá zahŕňa hudbu, filmy, video, knihy a spravodajské časopisy.

Cloudová infraštruktúra spoločnosti Google sa rovnako radikálne rozrastá. Investície spoločnosti Google do cloudovej infraštruktúry dnes prevyšujú investície spoločnosti Amazon. Na rozdiel od Amazonu sa spoločnosť Google venuje konkrétnym službám ako Gmail a Google Talk. Väčšina služieb Google je navyše bezplatná a sú podporované reklamami. Z pohľadu takéhoto modelu má spoločnosť Google veľa konkurentov v oblasti konkrétnych služieb. Napríklad v hudbe je najväčším konkurentom služby Google Play spoločnosť Apple iTune, ktorá je v tejto oblasti priekopníkom. V prípade ukladania súborov sú veľkými konkurentmi pre Disk Google služby Microsoft OneDrive a Dropbox, ktoré ponúkajú verejnosti bezplatné verzie služieb.

Spoločnosť Google mala v posledných rokoch taktiež nečakané výpadky v cloude, ktoré v niektorých prípadoch trvali až 30 hodín. Keďže milióny zákazníkov na celom svete využívajú Google Apps, aj malé prerušenie služby, napr. e-mailová nedostupnosť služby na 15 minút môže mať na zákazníkov významný negatívny dopad. Spoločnosť Google ponúka všetky tri základné typy cloudových služieb – SaaS, PaaS a IaaS. Jej popularita ako poskytovateľa cloudových služieb je podporovaná hlavnými službami, ako sú YouTube a Gmail. Od roku 2010 je prístupný elektronický obchod G Suite Marketplace (predtým Google Apps Marketplace) s ponukou firemných cloudových aplikácií, ktoré rozširujú existujúce možnosti Google Apps. Správcovia tu môžu prechádzať, nakupovať a zavádzať integrované cloudové aplikácie určené pre firmy [S14].

[11] https://about.google/intl/sk/products/



Obrázok 0-10 Ponuka produktov pre podnikanie od spoločnosti Google[12]

Microsoft Azure[13] *and Office 365*[14] – spoločnosť Microsoft ponúka cloudové služby pre rôzne modely – SaaS, PaaS a IaaS. Windows Azure, uvedený na trh v roku 2010, sa špecializuje na modely PaaS a IaaS. Microsoft Office 365 sa špecializuje na model SaaS z balíka produktov Microsoft Suite. Office 365 v kombinácii s programom OneDrive spoločnosti Microsoft umožňuje podnikovým zákazníkom ľahko zdieľať textové dokumenty, tabuľky a prezentácie medzi používateľmi v rozptýlených geografických lokalitách. Popularita cloudových služieb spoločnosti Microsoft je spojená aj s tým, že zamestnanci organizácií sú zvyknutí narábať s produktami spoločnosti Microsoft, predovšetkým s kancelárskym balíkom. Ako skutočná cloudová služba s globálnym dosahom poskytujú cloudové produkty spoločnosti Microsoft výhody škálovateľnosti, pružnosti dopytu a modelu pay-as-you-go. Rovnako ako ostatní poskytovatelia cloudových služieb, aj spoločnosť Microsoft zaznamenala niekoľko cloudových výpadkov.

Pretože Microsoft Azure podporuje databázové služby využívajúce SQL aj NoSQL, zákazníci majú možnosť spúšťať cez cloud rôzne databázové systémy. Windows Azure ponúka zákazníkom bezplatnú úroveň používania, ktorú si môžu najprv vyskúšať a potom sa prihlásiť na odber ďalších prémiových služieb, ktoré Azure ponúka. Vďaka úzkej integrácii platformy Azure s inými produktmi spoločnosti Microsoft, ako je napríklad Office 365, môžu zákazníci využívať model PaaS alebo SaaS pomocou jedného z produktov spoločnosti Microsoft.

[12] https://about.google/products/ > For business
[13] https://azure.microsoft.com/
[14] https://www.office.com/

Spoločnosť Microsoft vstúpila na cloudový trh oveľa neskôr v porovnaní s inými významnými poskytovateľmi cloudových služieb, ako sú Amazon a Google. Napriek tomu investície spoločnosti Microsoft do cloudovej infraštruktúry sú vyššie ako spoločnosti Amazon a cloud computing patrí medzi najrýchlejšie rastúce časti spoločnosti Microsoft a pomaly znižuje náskok AWS, najmä medzi podnikmi.

IBM Cloud[15] – spoločnosť IBM ponúka zákazníkom rôzne cloudové služby. Všetky ponuky sú navrhnuté na obchodné použitie pre podniky a predávajú sa pod názvom IBM SmartCloud. Cloud IBM obsahuje IaaS, SaaS a PaaS ponúkané prostredníctvom rôznych modelov nasadenia s vlastnými IBM značkovými službami. SmartCloud sa skladá z infraštruktúry, hardvéru, nasadenia, manažmentu, integrácie a zabezpečenia, ktoré slúžia ako základ privátneho alebo hybridného cloudu. Spolu s IaaS, PaaS a SaaS ponúka IBM tiež obchodný proces ako službu (BPaaS, business process as a service), či dokonca pristup k superpočítaču IBM Watson a Watson Assistant.

Cloudové služby IaaS poskytujú zákazníkom spracovanie, ukladanie, siete a ďalšie základné počítačové zdroje, v ktorých je zákazník schopný nasadiť a spustiť ľubovoľný softvér, ktorý môže zahŕňať operačné systémy a aplikácie. IBM Cloud dramaticky rozšíril výber softvéru, ktorý sa môže nachádzať na ich virtuálnych/fyzických serveroch. IBM ponúka 30 rôznych možností softvéru, vrátane CentOS, CloudLinux, Debian, Microsoft, cez hypervízory Brocade, Citrix, VMware, až po OS FreeBSD. PaaS cloudové služby umožňujú zákazníkom nasadiť do cloudovej infraštruktúry existujúce alebo vlastné aplikácie vytvorené zákazníkom pomocou programovacích jazykov a nástrojov podporovaných poskytovateľom. IBM sa špecializuje na vysoko pokročilé a prispôsobené dátové centrá, takže s touto službou je možné robiť aj špecializované operácie. SaaS cloudové služby umožňujú zákazníkom využívať aplikácie poskytovateľa, ktoré sú prevádzkované v cloudovej infraštruktúre. Aplikácie sú prístupné z rôznych klientskych zariadení prostredníctvom tenkého klientskeho rozhrania, ako je napríklad webový prehľadávač (napr. webový e-mail). Cloudové služby obchodných procesov sú akékoľvek obchodné procesy (horizontálne alebo vertikálne) poskytované prostredníctvom modelu cloudových služieb (multitenant, samoobslužné poskytovanie služieb, elastické škálovanie a meranie spotreby alebo používanie cien) prostredníctvom internetu s prístupom cez webové rozhrania a využívajúce webové služby [MB16].

Oracle Cloud[16] – je služba cloud computingu ponúkaná spoločnosťou Oracle Corporation, ktorá poskytuje servery, úložiská, sieť, aplikácie a služby prostredníctvom globálnej siete dátových centier spravovaných spoločnosťou Oracle Corporation. Spoločnosť umožňuje poskytovanie týchto služieb na požiadanie prostredníctvom internetu. Oracle Cloud poskytuje model IaaS, PaaS, aj SaaS a podporný modul dáta ako službu (DaaS, Data as a Service). Tieto služby sa používajú na vytváranie, nasadzovanie,

[15] https://www.ibm.com/cloud
[16] https://www.oracle.com/

integráciu a rozširovanie aplikácií v cloude. Platforma podporuje množstvo otvorených štandardov (SQL, HTML5, REST atď.), open-source aplikácie (Kubernetes, Hadoop, Kafka, atď.) a množstvo programovacích jazykov, databáz, nástrojov a rámcov vrátane špecifického softvéru Oracle. Na vysoko konkurenčnom trhu cloud computingu spoločnosť Oracle obsadila svoje miesto tým, že vytvára riešenia, ktoré zodpovedajú potrebám konkrétnej skupiny zákazníkov. Predstavitelia Oracle radi zdôrazňujú nadradenosť spoločnosti Oracle nad AWS v rôznych aspektoch. Napríklad v roku 2016 uviedli, že „Amazon je o 20 rokov pozadu oproti Oracle v oblasti databázových technológií."

Oracle Cloud, tak ako AWS, poskytujú širokú škálu služieb a produktov. Okrem toho predajca poskytuje cloudové služby, t. j. aplikácie, middleware a databázu, ako integrovaný balík, čo vylučuje potrebu nákupu riešení tretích strán. Uvedené predstavuje jednu z jeho najdôležitejších výhod a výsledkom je používateľsky prívetivé prostredie. Navyše sa spoločnosť Oracle spolieha na špičkové technológie, vďaka ktorým je oveľa rýchlejšia a výkonnejšia ako jej konkurenčné riešenia, najmä pokiaľ ide o vysokokapacitné aplikácie. Rovnako výkonný modul DaaS umožňuje prepojiť databázové služby s PaaS a IaaS a umožňuje ich škálovateľnosť.

Na druhej strane, cloudové riešenia Oracle majú určité nevýhody, čo môže mnohé spoločností odradiť a zvolia si inú cloudovú platformu. Prvou nevýhodou je slabá ponuka pre základné vybavenie – keďže spoločnosť Oracle je zameraná na špičkové technológie, jej ponuka iba pre základnú úroveň je veľmi obmedzená.. Hoci Oracle poskytuje svoje služby a produkty hneď „po vybalení", poskytnuté riešenia nemusia postačovať pre spoločnosti, ktoré síce potrebujú jednoduché funkcie, ale tie v balíku nie sú implementované dostatočne; tobôž pre podniky, ktoré potrebujú komplexnú platformu.

Alibaba Cloud[17] – je popredným čínskym poskytovateľom cloudu, dcérska spoločnosť skupiny Alibaba. Alibaba Cloud poskytuje služby cloud computingu pre online podniky a vlastný ekosystém elektronického obchodu Alibaba. Medzinárodné prevádzky spoločnosti Alibaba Cloud sú registrované so sídlom v Singapure. Alibaba Cloud ponúka cloudové služby, ktoré zahŕňajú elastické výpočty, ukladanie údajov, relačné databázy, spracovanie veľkých dát, ochranu proti DDoS a siete na doručovanie obsahu (CDN, Content Delivery Networks). Mimo štatútu najväčšej spoločnosti v oblasti cloud computingu v Číne, Alibaba Cloud pôsobí v 19 oblastiach dátových centier a 56 zónach dostupnosti po celom svete a spoločnosť Gartner ju radí ako cloudovú infraštruktúru v rámci celého sveta. Jedným z hlavných nedostatkov je zatiaľ malá ponuka služieb a riziko zneužitia citlivých údajov s prepojením na vládu Čínskej republiky.

Dropbox[18] – Dropbox je priekopníckym poskytovateľom cloudových úložísk s viac ako 500 miliónmi zákazníkov na celom svete. Jedinou cloudovou službou, ktorú Dropbox

[17] https://www.alibabacloud.com/
[18] https://www.dropbox.com/

ponúka, je úložisko a umožňuje používateľom ukladať a zdieľať súbory a priečinky s ostatnými používateľmi internetu pomocou synchronizácie súborov. Spravuje viac ako 10 000 serverov, aby uchovával metadáta súborov zákazníkov a na ukladanie skutočných súborov zákazníkov využíva službu AWS S3. Údaje naznačujú, že zákazníci nahrávajú 1 miliardu súborov denne. Veľká zákaznícka základňa je spôsobená dostupnosťou 2 GB voľného úložného priestoru, ktorý je možné upgradovať na 100 GB za ročný poplatok. Dropbox poskytuje 256-bitové šifrovanie pre dáta pomocou AES. Pretože skutočné súbory sa ukladajú na AWS, Dropbox ťaží z vysokej dostupnosti a spoľahlivosti AWS pre prístup k súborom zákazníkov. Dropbox neidentifikoval príčiny výpadkov, ktoré nastali v posledných rokoch, čo znižuje dôveru zákazníkom v službu.

Dropbox má vážnu konkurenciu v službe Disk Google od spoločnosti Google a v službe OneDrive od spoločnosti Microsoft. Dropbox zjednodušil proces ukladania a prístupu vývojom API, ktoré si zákazníci môžu stiahnuť a nainštalovať na svoje počítače. Okrem toho slúži priečinok na pracovnej ploche ako odkaz na Dropbox, čo používateľom uľahčuje jednoducho presunúť svoje súbory do priečinka na pracovnej ploche a uložiť ich do cloudu. Dropbox sa automaticky synchronizuje na pozadí so zákazníckymi zložkami s cloudovým úložiskom. Vďaka ľahkému používaniu sa služba stala populárnou. Služba je navyše k dispozícii na všetkých troch hlavných platformách – MS Windows, Mac a Linux. Dropbox umožňuje zákazníkom prístup k uloženým súborom na akomkoľvek zariadení vrátane mobilných zariadení, či prostredníctvom webového rozhrania.

Pre väčšiu bezpečnosť môže zákazník ukladať súbory s heslom. Ako už bolo uvedené, Dropbox nevlastní svoju infraštruktúru na ukladanie súborov, pretože ju spracúva AWS S3. Jedinou funkciou zabezpečenia, ktorú Dropbox uvádza je prenášanie a ukladanie všetkých dát v šifrovanej podobe. Nedostatočná podpora iných bezpečnostných mechanizmov je jedným z hlavných dôvodov, prečo niektoré firmy uprednostňuje iných dodávateľov úložných služieb. Kontrola prístupu k súboru v službe Dropbox je oveľa jednoduchšia v porovnaní s tradičným prístupom FTP. S odkazom poskytnutým vlastníkom súboru je možné priamo pristupovať k súboru bez akejkoľvek ďalšej autentifikácie [S14].

Apple iCloud[19] – je cloudová služba od spoločnosti Apple integrovaná do všetkých zariadení spoločnosti. Idea iCloudu je postavená na filozofii, že používateľský obsah je uložený na serveri spoločnosti Apple a používateľ môže tieto dáta synchronizovať a meniť. iCloud podporuje základné aplikácie od spoločnosti Apple, akými sú Kontakty, Kalendár, Mail alebo iTunes. Popritom Apple ponúka aj vývojárske nástroje, ktoré možno použiť pre začlenenie iCloudu do aplikácií tretích strán. Oproti iným službám typu cloud má iCloud tú výhodu, že je integrovaný na úrovni operačného systému ako takého a používateľ sa na využívanie iCloudu nemusí nikde registrovať, postačuje mu Apple ID.

[19] https://www.icloud.com/

Avšak podnikové nasadenia iCloudu ako plnohodnotného cloudového riešenia nie je ešte komplexné, iCloud sa zatiaľ využíva skôr ako doplnok podnikovej sady nástrojov.

VMware Cloud on AWS[20] – služba manažovaná spoločnosťou VMware umožňuje firmám spúšťať svoje aplikácie v privátnych, verejných alebo hybridných cloudových prostrediach založených na VMware s optimalizovaným prístupom k celej šírke služieb AWS. Spoločnosť VMware spolupracuje s firmou AWS na vytvorení plne spravovaného prostredia VMware v cloude AWS pomocou nástrojov VMware, ako sú vSphere, vSAN, NSX a vCenter. Cieľom VMware Cloud on AWS je pomocou nástrojov VMware aplikovaných na verejný cloud AWS efektívne vytvoriť hybridné prostredie bez toho, aby bol lokálne vytvorený privátny cloud. VMware a AWS ponúkajú od mája 2019 VMware Cloud on AWS vo väčšine hlavných regiónov AWS.

Navyše, používatelia môžu využívať VMware Cloud on AWS bez akýchkoľvek lokálnych produktov VMware a môžu službu prevádzkovať, napríklad iba prostredníctvom pripojenia webového prehliadača k účtu AWS. Na druhej strane, čím viac komponentov VMware už beží v lokálnom dátovom centre, tým ľahšie je rozšíriť tieto nástroje na cloud AWS. Správcovia môžu používať nástroje, ako napríklad vMotion, na zjednodušenie migrácie svojich virtuálnych strojov v podniku na AWS cloud.

Medzi VMware Cloud on AWS a lokálnymi nasadeniami nástrojov VMware existujú určité dôležité rozdiely. Používatelia VMware Cloud on AWS majú prístup k známym nástrojom vSphere a súčasne ťažia z výhod verejného cloudu AWS. VMware technológie ako VMware NSX, čo je platforma pre virtualizáciu sietí, umožňujú prevádzkovať celý sieťový a bezpečnostný model vo forme softvéru, oddelene od sieťového hardvéru a bezpečné pripojenie k Amazon Virtual Private Cloud. Na druhej strane, VMware Cloud on AWS je spravovaná služba, VMware spravuje a prevádzkuje infraštruktúru, takže správcovia neinštalujú ani nekonfigurujú základné ESXi, NSX alebo vSAN. Služba sa tiež stará o opravy a nápravu porúch hardvéru. Dôsledkom je strata určitej kontroly nad virtualizačnými vrstvami. Pre niektorých to môže byť prijateľný kompromis, zatiaľ čo iní môžu používanie infraštruktúry ako „čiernej skrinky“ odmietnuť a spravovať iba svoje virtuálne počítače, kde nástroje VMware umožňujú administratívnu kontrolu produktu. Navyše VMware Cloud on AWS neponúka úplnú funkcionalitu ako lokálne nástroje VMware a aj cenová politika je iná.

Tabuľka 0-1: Zhrnutie hlavných poskytovateľov cloudových služieb.

Poskytovateľ	**Typ služby**	**Názov produktu**
Amazon	SaaS	AWS
	PaaS	AWS Elastic Beanstalk
	IaaS	EC2, Amazon S3

[20] https://cloud.vmware.com/vmc-aws

Google	SaaS	Gmail, GoogleDocs
	PaaS	Google App Engine
	IaaS	Google Compute Engine
Microsoft	SaaS	Office 365, Azure SaaS
	PaaS	Azure Platform/Web Apps
	IaaS	Azure infrastructure
IBM	SaaS	CloudBurst
	PaaS	IBM Cloud
	IaaS	IBM Cloud
Oracle	SaaS	Oracle Cloud Applications
	PaaS	Oracle Cloud Platform
	IaaS	Oracle Cloud Infrastructure
Dropbox	SaaS	Dropbox
Apple	SaaS	iCloud
VMware	IaaS	vCloud Director