
Prínosy a riziká cloud computingu

Pavol Jurík¹

Abstrakt

Cloud computing je v súčasnej dobe populárny spôsob poskytovania a používania IT služieb. Jeho popularita narastá najmä preto, že jeho použitie môže používateľom priniesť úsporu finančných nákladov súvisiacich s vývojom, prevádzkou a aktualizáciou aplikácií a tiež s nákupom, prevádzkou a údržbou výpočtových zdrojov, ako sú operačné pamäte, procesory, servery, dátové úložiská a pod. Používateľmi pritom môžu byť jednotlivci, firmy, ale aj organizácie vo všeobecnosti (napr. škola, úrad a pod.), a tak majú technológie cloud computingu pomerne široké možnosti uplatnenia. Napriek nesporným výhodám má však použitie takýchto technológií aj svoje tienisté stránky. Cieľom tohto článku je preto identifikovať a charakterizovať hlavné prínosy a tiež hlavné úskalia zavádzania cloud computingových služieb do technologickej architektúry podnikových informačných systémov. Vďaka tomu môže článok poslúžiť ako pomôcka pre firmy a ich manažérov pri rozhodovaní sa o použití alebo nepoužití takéhoto riešenia.

Kľúčové slová

Cloud computing, SaaS, PaaS, IaaS, technologická platforma, IT infraštruktúra

Abstract

Nowadays, Cloud Computing is a popular way of providing and using IT services. Its popularity is growing mainly because of the fact that its usage can bring savings of financial costs related to the development, operation and actualisation of applications and also costs related to the purchase, operation and maintenance of computing resources, such as operating memories, CPUs, servers and data storages to the user. Not only individuals, but also companies and organisations in general (for example schools, administrative departments, etc.) can be considered as users and because of that Cloud Computing technology has got a fairly wide applicability. However, despite of these undeniable advantages the usage of this technology has got also its downsides. The aim of this article is therefore to identify and characterize the main benefits and also the main pitfalls of the inclusion of Cloud Computing services into technological architecture of business information systems. Because of that this article can serve as an aid for companies and their managers who are interested in the usage of this technology in their choice of using it or not.

Key words

Cloud computing, SaaS, PaaS, IaaS, technological platform, IT infrastructure

JEL classification

L86

1 Úvod

Cloud computing je služba, ktorá umožňuje podnikom, organizáciám a jednotlivcom využívať výpočtové zdroje (napr. aplikácie, operačné systémy, hardvér, platformy, dátové úložiská a pod.) na diaľku prostredníctvom internetu od externých poskytovateľov. Zvyčajne je

¹Ing. Pavol Jurík, PhD., Ekonomická univerzita v Bratislave, FHI, KAI, Dolnozemska cesta 1/b, 852 35 Bratislava, e-mail: pavol.jurik.euba@gmail.com.

táto služba platená, no v niektorých prípadoch ju poskytovateľ pre používateľov sprístupňuje zadarmo (príkladmi takýchto služieb sú Google Disk, Microsoft OneDrive a pod.).

Firmy sa môžu rozhodnúť, či budú celý svoj informačný systém (tzn. všetky aplikácie v rámci neho, všetky servery, dátové úložiská, operačné systémy a pod.) prevádzkovať na vlastnej technologickej infraštruktúre, teda vo vlastnej réžii alebo pritom využijú cloud computingové služby externých poskytovateľov. Služby cloud computingu nemusia pokrývať celý informačný systém v plnom rozsahu, ale môžu slúžiť len na zabezpečenie niektorých čiastkových oblastí, ako sú prevádzka konkrétnej aplikácie, resp. aplikácií, prevádzka dátového úložiska pokrývajúceho len určitú podmnožinu podnikových alebo organizačných údajov a pod. Technologická infraštruktúra určitého podniku alebo organizácie teda môže byť riešená sčasti na báze vlastných prostriedkov a sčasti pomocou prostriedkov sprístupnených na báze cloudu.

Existujú tri základné modely cloud computingu (Apprenda, 2017):

- **SaaS** (*Software as a Service*) – používateľ (firma, organizácia, jednotlivec) má na diaľku prostredníctvom svojho webového prehliadača a pripojenia na internet zabezpečený prístup k aplikácii, ktorá je prevádzkovaná externým poskytovateľom cloudových služieb. Používateľ tak nemusí niesť počiatočné náklady na nákup softvéru, nemusí si ho nainštalovať, zabezpečovať jeho spravovanie, aktualizácie, riešenie chybových stavov a pod. K aplikácii má prostredníctvom služby SaaS zabezpečený prístup výlučne cez webový prehliadač s tým, že táto aplikácia je v plnom rozsahu prevádzkovaná na strane poskytovateľa. V prípade jednotlivcov môže ísť najmä o aplikácie typu poštového klienta (napr. Gmail, Centrum a pod.), online hry alebo aj profesionálne orientované aplikácie (napr. Corel Draw). U firiem a organizácií môžu byť na tejto báze používané rôzne typy aplikácií zamerané na podporu, evidenciu a plánovanie podnikových procesov (napr. aplikácie typu ERP, CRM a pod.). Aplikácie pre osobné potreby jednotlivcov sú obvykle poskytované zadarmo, pretože ich poskytovateľ má príjmy vyplývajúce z toho, že prostredníctvom týchto aplikácií poskytuje priestor na reklamu iným firmám. Aplikácie slúžiace na komerčné účely bývajú zasa zvyčajne poskytované za poplatok, ktorý zodpovedá rozsahu poskytovaných služieb, tzn. frekvencii a miere používania danej aplikácie.
- **PaaS** (*Platform as a Service*) – táto služba je zameraná na poskytovanie platformy slúžiacej na vývoj vlastných aplikácií na diaľku prostredníctvom webového prehliadača a pripojenia na internet. Používateľ teda nemusí investovať finančné prostriedky do vybudovania a správy vývojárskych platforiem umožňujúcich návrh, naprogramovanie a otestovanie vlastných aplikácií. Takúto platformu prevádzkuje poskytovateľ, ktorý okrem toho zabezpečuje aj prevádzku, údržbu, aktualizáciu, bezpečnosť a dostupnosť aplikácií vytvorených používateľom prostredníctvom tejto platformy. Firma, ktorá využíva služby PaaS teda nemusí mať vo vlastníctve svoje vlastné servery, softvér na vývoj aplikácií, nemusí zamestnávať svojich vlastných databázových administrátorov a ani sieťových špecialistov. Musí mať len vývojárov (analytikov, programátorov, testerov a pod.), ktorí sú schopní prostredníctvom na diaľku poskytovanej platformy vyvinúť želanú aplikáciu a tiež pracovníkov, ktorí ju budú používať.
- **IaaS** (*Infrastructure as a Service*) – je služba, ktorá je zameraná na poskytovanie výpočtových zdrojov na diaľku prostredníctvom pripojenia na internet. Týmito zdrojmi sú najmä servery, sieťové zariadenia, operačné pamäte, cykly procesora a priestor na ukladanie dát. Používateľ teda môže mať prostredníctvom tejto služby priamy prístup k serveru, ktorý sa fyzicky nenachádza v jeho bezprostrednom okolí, ale je umiestnený na inom geografickom mieste. Za chod, údržbu a bezpečnosť servera nesie zodpovednosť poskytovateľ. Rovnako môže používateľ využiť operačnú pamäť a procesorový výkon poskytovateľa v období, kedy si to jeho aplikácie vyžadujú (extrémne alebo nadštandardné prevádzkové zaťaženie v porovnaní s bežným obdobím), prípadne využiť externé

dátové úložisko prevádzkované na strane poskytovateľa. Vo všetkých týchto prípadoch používateľ ušetrí finančné prostriedky potrebné na nákup a prevádzkovanie príslušných výpočtových zdrojov s tým, že tieto zdroje sú mu sprístupnené na základe prenájmu, resp. poplatku zodpovedajúceho miere ich používania.

Existujú však aj ďalšie formy cloud computingu, resp. bližšie konkretizácie vyššie uvedených foriem, medzi ktoré patria najmä:

- **BaaS** (*Back-Up as a Service*) – ide o službu, pri ktorej je zodpovednosť za pravidelné zálohovanie podnikových údajov a tiež za bezpečnosť všetkých záloh presunutá na externého poskytovateľa. IT oddelenie podniku tak môže byť odbremenené od starostí súvisiacich so zálohovaním.
- **CaaS** (*Communication as a Service*) – ide o poskytovanie softvéru a hardvéru potrebného na zabezpečovanie komunikačných služieb externým poskytovateľom, a to najmä so zameraním na služby typu VoIP (z angl. Voice over Internet Protocol), okamžité posielanie textových správ (z angl. instant messaging) a videokonferenčné služby. Služby typu VoIP sú zamerané na prenos hlasu cez internet v reálnom čase tak, aby komunikujúce strany mali pocit, že prenos prebieha súvisle bez prerušenia.
- **DaaS** (*Desktop as a Service*) – ide o formu virtualizácie osobných počítačov, ktorá je zabezpečovaná externým poskytovateľom. Pri tejto virtualizácii sa celý obsah osobného počítača (súbory, údaje, programy, adresárová štruktúra a pod.) nakopíruje na externý server poskytovateľa, vďaka čomu môže používateľ pristupovať k obsahu svojho počítača na diaľku z ľubovoľného iného počítača, a to prostredníctvom svojho webového prehliadača. Obsah osobného počítača tak nie je viazaný na konkrétne zariadenie a je prístupný zo servera, na ktorý sa dá pripojiť z ľubovoľného zariadenia disponujúceho podporovanou verziou webového prehliadača.
- **DBaaS** (*Database as a Service*) – ide o služby, ktoré sa zameriavajú na poskytovanie externého dátového priestoru, jeho spravovanie, ako aj na poskytovanie monitorovacích a analytických nástrojov pracujúcich nad príslušnou databázou.
- **TaaS** (*Testing as a Service*) – ide o poskytovanie testovacích služieb na diaľku od externého poskytovateľa, zameraných najmä na testovanie výkonnosti alebo bezpečnosti rozličných aplikácií.
- **STaaS** (*Storage as a Service*) – ide o poskytovanie dátového úložiska určitej firme alebo jednotlivcovi na diaľku externým poskytovateľom. Nie je to však taká komplexná služba ako DBaaS, ktorá na rozdiel od STaaS zahŕňa aj monitorovacie a analytické nástroje.

Cloud computingové služby môžu byť poskytované štyrmi spôsobmi:

- **Verejný cloud** (*public cloud*) – ide o najčastejšie využívaný a najviac známy model poskytovania cloud computingových služieb. Služby typu SaaS, PaaS a IaaS (vrátane ich rôznych odnoží) sú v tomto prípade poskytované špecializovanou firmou, obvykle pôsobiacou na globálnom trhu prostredníctvom internetu, a to každému, kto má záujem o ich využívanie. Poskytovateľ sa obvykle usiluje o zabezpečenie vysokej škálovateľnosti (z angl. *scalability*), a to znamená, že používateľ nemusí danú službu používať v stále konštantnom rozsahu, ale môže mieru jej používania prispôbovať svojim aktuálnym potrebám. Miera používania určitej služby konkrétnym používateľom sa teda môže zvyšovať alebo znižovať v závislosti od jeho požiadaviek, a tomu zodpovedá aj adekvátne zvyšovanie alebo znižovanie poplatkov. Pre verejný cloud je typické to, že poskytovatelia si ponechávajú právo na zmenu rozsahu poskytovaných služieb.
- **Súkromný cloud** (*private cloud*) – ide o poskytovanie tých istých služieb, ako v prípade verejného cloudu, no s tým rozdielom, že tieto služby sú poskytované iba jednej

konkrétnej firme alebo organizácii, a to buď v jej vlastnej réžii alebo externou firmou. Vo vlastnej réžii môžu byť cloud computingové služby poskytované najmä vtedy, ak ide o veľké spoločnosti s viacerými pobočkami, resp. závodmi, pôsobiacimi vo viacerých mestách, príp. štátoch (jedna pobočka poskytuje služby ostatným pobočkám v rámci tej istej firmy). Súkromný cloud ponúka obvykle v porovnaní s verejným cloudom zvýšenú spoľahlivosť a bezpečnosť poskytovaných služieb, no tieto výhody idú na úkor vyšších poplatkov spojených s ich využívaním. Podobne, ako vo verejnom cloude, aj v súkromnom cloude je pre používateľa veľmi dôležitá možnosť dostatočnej škálovateľnosti využívaných služieb.

- **Hybridný cloud** (*hybrid cloud*) – ide o kombinované riešenie, pri ktorom môže určitá firma alebo organizácia naraz využívať služby verejného a súkromného cloudu tak, že tieto služby sa navzájom dopĺňajú a vytvárajú tak jeden celok. Výhodou takéhoto riešenia je možnosť uchovávať a spravovať citlivé dáta vo vlastnej réžii (v rámci súkromného cloudu poskytovaného jednou z pobočiek danej firmy alebo organizácie) a s ostatnými dátami pracovať v rámci verejného cloudu poskytovaného externou firmou.
- **Komunitný cloud** (*community cloud*) – ide o model, pri ktorom sú cloud computingové služby poskytované len subjektom v rámci určitej presne definovanej komunity (zoskupenie participujúcich firiem alebo organizácií so spoločným cieľom). Podobne, ako v prípade súkromného cloudu, aj pri tomto type poskytovania informačno-komunikačných služieb dochádza obvykle k značnej spolupráci medzi poskytovateľom a používateľmi, v dôsledku čoho sú tieto služby upravované a dimenzované podľa ich individuálnych požiadaviek.

2 Prínosy vyplývajúce z používania cloud computingových služieb

V tejto kapitole sa pokúsime naformulovať hlavné dôvody pre zavádzanie cloud computingu do technologickej architektúry podnikových informačných systémov. Tieto dôvody charakterizujeme v nasledujúcich podkapitolách.

2.1 Ekonomické prínosy

Po analýze podstaty cloud computingu je zrejmé, že najväčším dôvodom pre jeho zavádzanie sú vysoké počítačové investície, ktoré je potrebné vynaložiť pri budovaní vlastnej podnikovej IT infraštruktúry. Ak sa podnik rozhodne celú technologickú platformu, potrebnú pre chod informačného systému, vybudovať výlučne na svojich vlastných zdrojoch (teda tzv. *in-house*), potom musí zabezpečiť nákup, prevádzku a údržbu serverov, dátových úložísk, operačných systémov (potrebných pre beh jednotlivých aplikácií v rámci informačného systému), sieťovej infraštruktúry a podobne. S tým súvisí množstvo finančne náročných problémov, ako napr. potreba vybudovania a správy dodatočných dátových úložísk (ak kapacity existujúcich úložísk z prevádzkových dôvodov už nie sú dostatočné), energetická náročnosť údržby takýchto úložísk (chladenie, odvetrávanie, záložné zdroje energie a pod.), využiteľnosť kapacity serverov (napriek vysokým nákladom na nákup a prevádzku serverov nie sú tieto servery využívané nepretržite a naplno), náklady na nákup, resp. vývoj, ako aj prevádzku, aktualizáciu a údržbu aplikácií pokrývajúcich jednotlivé funkčné a procesné oblasti podniku a iné. Okrem toho je potrebné zamestnávať IT špecialistov, ktorí sú schopní vybudovať a udržiavať celú technologickú infraštruktúru komplexného informačného systému podniku a zabezpečiť jeho bezproblémový chod.

Pri použití cloud computingu však nastáva úspora finančných prostriedkov najmä z toho dôvodu, že podnik nemusí zabezpečovať nákup, prevádzku a údržbu všetkých komponentov informačného systému vo vlastnej réžii, ale môže určitú časť zodpovednosti a aj s tým súvisiacich nákladov preniesť na externú firmu. Poplatky za používanie cloudových služieb sú nižšie než

náklady, ktoré by bolo potrebné vynaložiť na zabezpečenie zodpovedajúcich služieb prostredníctvom vlastných výpočtových, softvérových a personálnych prostriedkov.

V prípade, ak ide o súkromný cloud zabezpečovaný vo vlastnej réžii určitej firmy alebo organizácie, vzniká úspora z toho dôvodu, že zodpovednosť za chod vybraných komponentov informačného systému ako celku preberá na seba iba jedna z pobočiek, ktorá zabezpečuje nákup, resp. vývoj, prevádzku a údržbu vybraných komponentov informačného systému pre všetky ostatné pobočky patriace danému podniku. Vďaka tomu podnik nemusí zamestnávať množstvo IT špecialistov vo všetkých pobočkách, ale môže väčšinu z nich sústrediť iba v jednej zo svojich pobočiek.

2.2 Technické prínosy

Prenesením časti zodpovednosti za nákup, prevádzku a údržbu niektorých komponentov informačného systému podniku na externé subjekty dochádza z pohľadu daného podniku k zjednodušeniu týchto procesov. Tým dochádza k odbremeneniu IT pracovníkov a k sprehľadneniu situácie vo vnútri informačného systému. Podnik tak môže ušetrené finančné prostriedky vynakladať do skvalitňovania iných oblastí súvisiacich s podnikaním, ako sú napr. marketingová kampaň, výskum a vývoj ako súčasť zdokonaľovania produktov, kontrola efektívnosti interných procesov podniku a pod.

Ďalším prínosom cloud computingu v oblasti techniky je to, že externí poskytovatelia sú obvykle schopní zabezpečiť vysokú mieru škálovateľnosti ponúkaných služieb. Počas prevádzky informačného systému sa totiž menia nároky na výkon serverov, kapacity operačných pamätí, výkonové charakteristiky procesorov, kapacity dátových úložísk a pod. Ak sa manažment podniku chce pripraviť na situácie, kedy budú prevádzkové nároky veľmi vysoké, musí si zaobstaráť vysoko výkonné výpočtové zdroje, ktoré by však v časoch nižších prevádzkových nárokov nedokázal efektívne využiť. Poskytovatelia cloudových služieb však obvykle môžu v prípade zistenia vyšších nárokov zo strany určitého používateľa pripojiť dodatočné výpočtové zdroje a v prípade neskoršieho zníženia nárokov môžu tieto zdroje opäť odpojiť, resp. ich prideliť iným používateľom.

2.3 Prínosy v oblasti mobility

Cloud computing sprístupňuje aplikácie a výpočtové zdroje pre používateľov prostredníctvom webového rozhrania. Používateľ teda pre prácu s nimi potrebuje len webový prehliadač a zariadenie, ktoré je schopné využiť všetku potrebnú funkcionálnosť tohto prehliadača. Nemusí ísť pritom len o stolový počítač, ale aj o notebook, netbook, tablet či dostatočne výkonný smartfón. Zamestnanec teda nie je viazaný na konkrétne zariadenie alebo konkrétne geografické miesto a môže byť pri využívaní cloud computingových služieb mobilný.

Vďaka tomu môže napr. obchodný zástupca firmy na rokovaní s obchodnými partnermi použiť určitú aplikáciu, získať z nej potrebné dáta a na základe toho urobiť operatívne obchodné rozhodnutie priamo na mieste. Okrem toho podporuje cloud computing aj zamestnávanie zamestnancov pracujúcich z domu (tzv. homeworking alebo teleworking), vďaka čomu môže zamestnávateľ ušetriť náklady, ktoré by inak bolo potrebné vynaložiť na zabezpečenie pracovného priestoru a podmienok pre týchto zamestnancov priamo v budove firmy (spotreba energií, nákup potrebného počítačového vybavenia, prenájom priestorov a pod.).

3 Riziká spojené s používaním cloud computingových služieb

V predchádzajúcej kapitole sme sa zaoberali prínosmi vyplývajúcimi z používania IT služieb na báze cloud computingu. Okrem týchto prínosov však existujú pri použití takýchto technológií aj viaceré riziká, ktoré nie sú zanedbateľné a podnik by ich mal starostlivo zvážiť. Tieto riziká si charakterizujeme v nasledujúcich podkapitolách.

3.1 Ochrana dát

Pravdepodobne najviac skloňovanou obavou v súvislosti s cloud computingom je neistota v súvislosti s ochranou dát. Pokiaľ je celý informačný systém určitého podniku postavený len na jeho vlastnej technologickej infraštruktúre a všetky dáta sú uložené výlučne v interných dátových úložiskách, potom má tento podnik nad svojimi dátami relatívne vysoký stupeň kontroly a môže dohliadať na ich ochranu (aj keď nie je možné vylúčiť stratu dát v dôsledku internej technickej chyby alebo zámerným pričinením niektorého zo zamestnancov). Pokiaľ sú dáta uchovávané a spracovávané len v rámci intranetu a neprechádzajú cez internet, minimalizuje to možnosti „útok zvonka“. Cloud computing je však principiálne postavený na tom, že dáta sú medzi poskytovateľom a používateľom určitej služby prenášané prostredníctvom internetu, a preto môžu byť potenciálne zachytené hackermi s cieľom ublížiť danému podniku a poskytnúť tieto dáta konkurencii, príp. môže ísť o konkurenciu samotnú (Bartošek, Petrucha, 2010).

Okrem obáv súvisiacich s tým, že dáta používateľov cloudových služieb sa môžu dostať k iným osobám, než k tým, pre ktoré sú určené, sa objavujú tiež obavy týkajúce sa toho, či tieto dáta nemôžu byť nežiaducim spôsobom modifikované počas prenosu po verejnej sieti v dôsledku zlyhania hardvéru alebo softvéru. V tejto súvislosti je veľmi dôležitá nielen úroveň zabezpečenia dátovej bezpečnosti na strane poskytovateľa, ale aj úroveň a kvalita zabezpečenia klientskych aplikácií (teda aplikácií na strane používateľov).

Klientske aplikácie si zvyknú ukladať údaje o používateľských účtoch, ktoré do nich boli zadané ich používateľmi. Ak nie sú dostatočne zabezpečené, môžu sa stať cieľom útoku hackerov, ktorí sa takto môžu dostať k dátam o používateľských účtoch, následne ich zmeniť, a tak zamedziť používateľovi v ďalšom používaní jeho účtu. Prípadne môžu používateľské kontá potajme používať bez modifikácie pôvodných prihlasovacích údajov a sledovať tak činnosť používateľa v danej aplikácii bez jeho vedomia. Nebezpečenstvo môže tiež predstavovať synchronizácia údajov, pretože útočník môže po získaní prihlasovacích údajov nastaviť automatické kopírovanie, resp. zálohovanie údajov súvisiacich s používaním danej aplikácie jej legitímnym používateľom na záznamové médium útočníka, ak takúto možnosť príslušná aplikácia podporuje.

Pri využívaní IT služieb na báze cloud computingu sú údaje používateľov nahraté v externých dátových centrách s tým, že títo používatelia nemajú žiadnu kontrolu nad tým, ako poskytovateľ príslušnej služby s týmito údajmi narába. Poskytovatelia sa obvykle zaručujú, že dáta ich klientov neposkytnú tretím stranám a vytvoria maximálne možné podmienky pre ich ochranu, no napriek tomu je otázne, do akej miery sa dá týmto tvrdeniam veriť.

Okrem toho však môžu nastať situácie, kedy sú poskytovatelia cloud computingových služieb povinní poskytnúť údaje nachádzajúce sa na určitom dátovom serveri štátnym inštitúciám. Ide o tieto prípady (Allen, Overy, 2014):

- žiadosti vydané súdmi alebo orgánmi činnými v trestnom konaní pre účely vedenia súdneho konania alebo vyšetrovania,
- žiadosti vydané daňovými orgánmi za účelom určenia alebo výberu daní alebo ciel,
- žiadosti vydané bezpečnostnými a informačnými službami za účelom výkonu im zverených úloh.

Ako uvádza Schmidt: „k takýmto prípadom dochádza pomerne často pri serveroch umiestnených na území USA. Takáto situácia môže nastať v prípade porušenia zákonov, podozrenia z porušovania autorských práv, prípadne podozrenia zo šírenia nelegálneho obsahu. Fungovanie cloudu vďaka distribúcii údajov nebýva ovplyvnené, avšak údaje sa dostanú k analytikom, ďalej sa spracovávajú a citlivé informácie sa môžu objaviť vo vyšetrovacích spisoch, alebo sa môžu dostať do nepovolaných rúk.“ (Schmidt, 2016).

3.2 Dostupnosť služieb

Okrem obáv o bezpečnosť údajov umiestnených v cloude sa objavujú aj obavy súvisiace s dostupnosťou poskytovaných služieb. Tieto obavy sa týkajú toho, či bude služba používaná na báze cloud computingu skutočne dostupná vždy, keď ju dotyčný používateľ bude chcieť použiť, a teda či nebude dochádzať k výpadkom, príp. k obmedzeniam v rozsahu jej používania. Najmä u menších poskytovateľov cloudových služieb hrozí ich odchod z trhu v prípade neúspechu a s tým súvisí riziko ukončenia poskytovania danej služby.

Príkladom obmedzenia dostupnosti služby poskytovanej na diaľku je výpadok služieb Amazon Web Services (Amazon AWS), ktorý nastal 1. marca 2017 a trval niekoľko hodín. Počas tejto doby nemohli používatelia používať s tým súvisiace webové stránky a aplikácie. Výpadok sa týkal používateľov vo východnej časti USA (Javůrek, 2017).

Iným príkladom je masívny výpadok internetového vyhľadávača Google, ktorý nastal 16. novembra 2016 a znemožnil prístup k jeho službám pre milióny používateľov v strednej Európe (vrátane Slovenskej a Českej republiky). Okrem toho neboli dostupné ani služby YouTube, Google maps, Gmail, Google prekladač a ani sociálna sieť Google+ (Kadlec, 2016).

V prípade takýchto výpadkov môže ísť o internú chybu na strane poskytovateľa určitej služby, ale aj o cieľový hackerský útok. Medzi takéto útoky patria najmä útoky typu „Denial of Service“, resp. „Distributed Denial of Service“, pri ktorých sa útočníci usilujú o znefunkčenie vybranej služby prostredníctvom zaplavenia servera sústavným prúdom paketov, v čoho dôsledku je server zahŕtený a nie je schopný obsluhovať požiadavky legitímnych používateľov. Môže tak dôjsť k vyčerpaniu výpočtových zdrojov servera a k jeho následnému „zrúteniu“. Útok typu „Distributed Denial of Service“ je realizovaný prostredníctvom viacerých zariadení, ktoré paralelne vysielajú dáta, príp. ich vysielajú sériovo s veľmi malými časovými rozstupmi tak, aby bol cieľový server po určitý čas zahŕtený. Prostredníctvom takýchto útokov sa hackeri zväčša usilujú buď o svoje zviditeľnenie, alebo o nelegálne získanie finančných prostriedkov vo forme výkupného vyplateného za to, že na určitý podnik alebo inštitúciu nezrealizujú takýto útok. Rovnako môže ísť aj o spôsob konkurenčného boja medzi firmami pôsobiacimi na spoločnom trhu s cieľom presvedčiť zákazníkov o nespoľahlivosti konkurenčnej firmy a služieb ňou poskytovaných.

4 Záver

Cieľom tohto článku bolo identifikovať a charakterizovať hlavné prínosy a hlavné úskalia vyplývajúce zo zavádzania cloud computingových služieb do technologickej architektúry podnikových informačných systémov. Prínosy sme zhrnuli do troch hlavných bodov, ktorými sú:

- *ekonomické prínosy* – úspora finančných prostriedkov súvisiacich s vývojom, prevádzkou a aktualizáciou aplikácií a tiež s nákupom, prevádzkou a údržbou výpočtových zdrojov, ako sú operačné pamäte, procesory, servery, dátové úložiská a pod.,
- *technické prínosy* – odbremenenie interného IT oddelenia od technicky náročných procesov a činností, o ktoré sa postará externý poskytovateľ príslušnej služby,
- *podpora mobility* – možnosť používania vybraných IT služieb na rôznych miestach a prostredníctvom rôznych zariadení s využitím webového prehliadača.

Potenciálne hrozby súvisiace s používaním cloud computingových služieb sme zhrnuli do dvoch hlavných kategórií, a to:

- *riziko straty citlivých dát,*
- *riziko nedostupnosti používanej služby.*

Vzhľadom k tomu, že prínosy aj riziká súvisiace s používaním IT služieb na báze cloud computingu sú pomerne významné, nie je ľahké vysloviť pre potenciálneho používateľa konkrétne odporúčanie. Vo všeobecnosti môžeme povedať, že ak používateľ (či už ide o osobu, firmu, alebo organizáciu) pracuje s citlivými dátami, ktoré sú z jeho pohľadu veľmi významné a nemali by sa dostať do rúk iných osôb alebo subjektov, potom je pravdepodobne lepšie uchovávať a spravovať tieto dáta vo vlastnej režii. To isté platí aj o používaní aplikácií, resp. výpočtových prostriedkov, ktoré sú pre používateľa kľúčové a musia byť pre neho stále k dispozícii (používateľ si nemôže dovoliť občasnú nedostupnosť týchto služieb). Pre tie skupiny údajov, aplikácií a IT služieb vo všeobecnosti, ktoré sú pre používateľa menej významné a nemajú kľúčový dosah na jeho činnosť alebo záujmy, môže byť pre používateľa výhodné obrátiť sa na špecializovaných a dôveryhodných poskytovateľov cloud computingových služieb.

Literatúra

- [1] Allen & Overy. (2014). Cloud computing alebo ako právne zabezpečiť, aby sa nad Vašimi dátami nezamračilo. Retrieved March 8, 2017, from http://www.rackscale.sk/files/editor/allenoverey_cloud_computing.pdf.
- [2] Apprenda. (2017). IaaS, PaaS, SaaS (Explained and Compared). Retrieved March 4, 2017, from <https://apprenda.com/library/paas/iaas-paas-saas-explained-compared/>.
- [3] Bartošek, V., & Petrucha, R. (2010). Cloud Computing: moderní směr poskytování IT služeb. *Systémová integrace*, (1), 79-90. Retrieved March 8, 2017, from <http://www.cssi.cz/cssi/cloud-computing-moderni-smer-poskytovani-it-sluzeb>.
- [4] IBM. What Is Cloud Computing. Retrieved October 4, 2016, from <https://www.ibm.com/cloud-computing/what-is-cloud-computing>.
- [5] Javůrek, K. (2017, March 1). Cloud od Amazonu měl několik hodin problémy, způsobilo to výpadky velkých webů a aplikací. Retrieved March 7, 2017, from <http://connect.zive.cz/bleskovky/cloud-od-amazonu-mel-nekolik-hodin-problemy-zpusobilo-to-vypadky-velkych-webu-a-aplikaci/sc-321-a-186420/default.aspx>.
- [6] Jurík, P. (2016). *Informačné systémy v podnikovej praxi*. Nové Zámky, Slovensko: AZ Print, s. r. o.
- [7] Kadlec, R. (2016, November 22). Google mal výpadok. Vyhľadávač aj ostatné služby už fungujú (doplnené). Retrieved March 7, 2017, from <https://touchit.sk/google-aj-jeho-sluzby-maju-vypadok/83694>.
- [8] Schmidt, P. (2016). Bezpečnosť a ochrana údajov z pohľadu cloud computingu. *Ekonomika a informatika*, 14(2), 153-165. Retrieved March 8, 2017.