Ako vybrať správny „oblak“ pre firmu

Cloud computing je nový fenomén v oblasti IT, ktorý firmám ponúka zvýšenie flexibility práce s vnútornými dátami, a tak im umožňuje pozdvihnúť sa na vyššiu úroveň v oblasti informačných technológií. S príchodom virtualizácie dochádza k ustupovaniu riešenia firemnej siete cez lokálnu sieť. Virtualizácia umožňuje vytvorenie abstraktnej úrovne určenej na prácu s dátami. Cloud computing priniesol štyri základné modely nasadenia (nerátame vládny cloud) vzhľadom na ich použitie pri práci s údajmi firmy. Cieľom tohto článku je opísať tri najbežnejšie modely z hľadiska ich implementácie, architektúry a bezpečnosti. Tieto tri aspekty sú pre firmu dôležitým smerníkom pri výbere vhodného nasadenia. Najviac vyzdvihujeme bezpečnosť dát, keďže každá firma si chráni svoje vnútorné vlastníctvo a obáva sa straty, prípadne odcudzenia jej vnútorných dát. To je aj jedna z príčin, prečo sa firmy rozhodnú nevstupovať do cloudového riešenia. Vhodnosť, respektíve nevhodnosť, modelu pre firmu sme určili analýzou troch zložiek bezpečnosti – utajenia, integrity a dostupnosti dát. Za ukazovatele sme zvolili dostupnosť riadenia cloudu, spoľahlivosť, nároky pri zavedení modelu a bezpečnostné podmienky.

Dnešný technologický vývoj spôsobil nárast údajov, ktoré si vynútili pozornosť informatikov s cieľom zamerať sa na úložiská dát. Riešenie malo byť dostupné pre všetky firmy. Najdrahším, ale najjednoduchšie realizovateľným bolo ukladanie na lokálnej sieti (LAN). Výhodou LAN je vysoký výkon a dostupnosť ukladania dát cez ustálené rozhrania firiem. Životnosť serverov, nutnosť zálohovania a obnovy systému a kúpa licencií ukázali, že toto riešenie nebolo tým najsprávnejším.

Azda za zanedbateľnú nevýhodu by sme považovali fyzické umiestnenie siete. LAN je energeticky závislá, a tak vplýva aj na environmentálne problémy Zeme. Riešenie bolo potrebné odkloniť od fyzickej vrstvy. Cloud computing, tiež nazvaný green cloud, poskytuje lacné a prakticky neobmedzené úložisko údajov. Na zabezpečenie prístupu k dátam sa využíva internet (prípadne WAN). Označenie green cloud získal vďaka nižším energetickým potrebám a environmentálnej záťaži. K veľkým plusom cloud computingu môžeme zaradiť automatické zálohovanie a obnovu systému, ako aj to, že nepotrebuje fyzickú výmenu. Výrazným negatívom je rýchlosť, ktorá klesla z dôvodu využívania obmedzených pásiem. Ukladanie dát do cloudu je založené na sieťovom prepojení medzi LAN a poskytovateľom úložiska údajov v cloude. Jeho vysoká citlivosť na sieť (pri výpadku) môže spôsobiť úplnú nedostupnosť. Častým problémom s cloudom je aj konsolidácia s firmou.

Súkromný cloud sa chápe ako termín marketingu pre počítačovú architektúru, ktorá poskytuje hostované služby pre obmedzený počet ľudí za firewallom (Rouse, 2009). Riadi ho samotná firma. Buď ide o sieť, alebo o dátové centrum, ktoré využíva cloud computing technológiu, akou je virtualizácia. Model nasadenia verejného cloudu je založený na štandardnom modeli cloud computingu, v ktorom poskytovateľ služieb (provider) tvorí prostriedky. Prostriedkami rozumieme rôzne aplikácie a služby skladovania určené pre širokú verejnosť na internete. Verejný cloud môže byť voľne dostupný alebo sa platí vlastnosť cloudu – pay-per-use, teda platí sa iba za to, čo využijeme (Rouse, 2009).

Tretí model nasadenia je hybridný cloud. Je udržiavaný internými aj externými poskytovateľmi. Tento model sa nazýva hybridný práve preto, že ide o spojenie dvoch predchádzajúcich modelov. Hybridný cloud využíva najmenej jeden súkromný cloud a aspoň jeden verejný cloud. Poskytuje sa v dvoch verziách, a to tak, že predajca má privátny cloud a tvorí partnerstvo s poskytovateľom verejného cloudu, alebo poskytovateľ verejného cloudu tvorí partnerstvo s dodávateľom, pričom dodávateľ poskytuje privátnu cloudovú platformu. Hybridný cloud je cloudové prostredie, v ktorom firma niektoré zdroje spravuje a poskytuje vo vnútri firmy, pričom niektoré sú poskytované externe (Rouse, 2010). Všeobecnou úlohou modelov je odklon od bežných biznisových modelov k progresívnejším technológiám budúcnosti. Naším cieľom je porovnať a nájsť jednotlivé výhody modelov nasadenia v rámci realizácie vo firmách s ohľadom na bezpečnosť dát.

Metódy riešenia

Architektúra modelov nasadenia je zložená z troch hlavných činiteľov – poskytovateľa, používateľa a zo služby. Úlohou poskytovateľa je vytvoriť cloud vo svojej sieti a umožniť tak používateľovi prístup k dátam. Ak je poskytovateľ a používateľ tá istá firma, poskytovateľom sa stáva IT oddelenie. Z toho vyplýva, že cloud je vytvorený v rámci firmy. V opačnom prípade je používateľom nezainteresovaná osoba, čo sa týka práce so službami (prechádza cez poskytovateľa) a dáta sa stávajú dostupné verejnosti. Pri riešení architektúry modelov využijeme metódu porovnania troch činiteľov (poskytovateľ, používateľ, služby), čím dokážeme nielen rozlíšiť jednotlivé typy cloudov, ale aj benefity, respektíve nevýhody použitia v rámci firmy.

Pri implementácii cloud computingu existuje pre uvedené modely spoločný spôsob nasadenia, a to použitie virtualizačných technológií pre dátové centrum. Hybridný cloud umožňuje vďaka svojej zložitosti tri spôsoby realizácie, na ktoré sme sa zamerali.

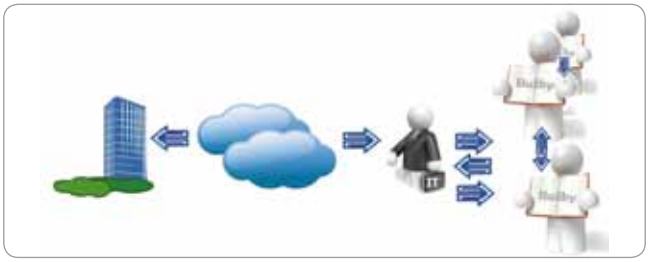
Bezpečnosť patrí k hlavným problémom cloud computingu. Pre dáta platia tri pravidlá bezpečnosti: utajenie, integrita a dostupnosť. Riešenie cez hybridný cloud je považované za najvhodnejšie v rámci bezpečnosti, ale je to skutočne tak? Môžu byť odlišné cloudy kompatibilné a zabezpečiť ochranu presunu dát z jedného oblaku do druhého? Ako dosiahnuť kompatibilitu týchto troch zložiek, opíšeme možným praktickým riešením.

Výsledky

Cloud ako výkonné hostingové riešenie reprezentuje model pay-as-you-go, ktorý umožňuje spoločnostiam škálovať ich infraštruktúru tak, aby zodpovedala rastu spoločnosti (Rybár, 2011). Teda výhoda použitia cloudu pre firmy spočíva v princípe platenia iba za to, čo firma použije.

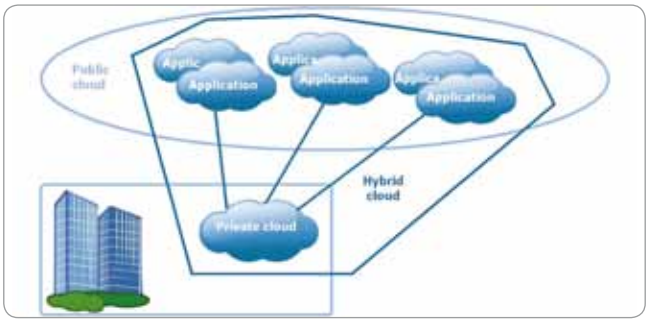
Za základný kameň architektúry cloud computingu sa považuje architektúra verejného modelu. Verejný cloud disponuje oproti virtuálnym serverom vysokou variabilitou, ale nízkym výkonom. Prístup k dátam je umožnený širokej verejnosti. V prípade firmy ide o prístup k mnohým klientom. Verejnosť sa stáva používateľom, ktorý neriadi cloud priamo, ale cez poskytovateľa. Poskytovateľom je firma, organizácia, ktorá spravuje služby.

Opakom verejného cloudu je súkromný cloud (obr. 1). Používateľ je súčasne aj poskytovateľ. Dátové centrum sa nachádza priamo vo firme a prístup je iba v rámci spoločnosti. Oddelenie pre informačné technológie firmy má za úlohu spravovať služby. Ak sa používateľom cloudu stane tretia osoba (iná firma, organizácia), cloud sa považuje za súkromný. Jeho škálovateľnosť je oproti verejnému a hybridnému cloudu výrazne ohraničená. Súkromný cloud sa považuje za najspoľahlivejší.



Obr. 1 Súkromný cloud

Medzi verejným a súkromným cloudom je hybrid (obr. 2). Navonok sa javí ako jeden cloud, avšak ide o prepletenú sieť najmenej jedného súkromného cloudu s niekoľkými verejnými oblakmi.



Obr. 2 Hybridný cloud

Hybridný cloud umožňuje firme stanoviť najlepšie formácie pre svoj biznisový model. Používateľ má transparentný prístup k dátovému centru, čo umožňuje jednoduchý pohyb medzi oblakmi. Vzťah medzi podnikom a poskytovateľom servisu je založený na princípe verejného aj súkromného cloudu. Do ich vzťahu vstupuje aj predajca cloudu, ktorý poskytne svoje ponuky firme. Úlohou poskytovateľa je vytvoriť hybridné cloudy a niekedy aj poskytnúť vlastné zásobníky (internal storage clouds).

Dáta vo verejnom cloude sú prístupné pomocou internetových protokolov REST (Representational State Transfer), v menšej miere ide o protokoly SOAP (Simple Object Access Protocol). Implementácia privátneho cloudu prebieha zavedením virtualizačnej technológie s integrovanými nástrojmi do dátového centra. Pre lepšiu názornosť sme sa rozhodli danú realizáciu opísať na príklade použitia platformy Hyper-V od Microsoftu. Hyper-V Cloud obsahuje programy nástrojov a metodík s cieľom implementácie privátneho cloudu do dátového centra. Hyper-V Cloud Deployment Guides obsahuje súbor nástrojov a postupov pre vytváranie privátnych cloudov pri využití existujúcej infraštruktúry. Hyper-V Cloud Accelerate je metodika zavádzania cloudových riešení. Providerom služieb je Hyper-V Cloud Service Provider Program. Využíva sa architektúra hypervízorov.

Pri implementácii hybridného cloudu treba splniť určité podmienky. Jednu z podmienok sme už uviedli pri architektúre – virtuálna transparentnosť. Takýto prístup k úložisku je umožnený, iba ak je cloud homogénny (homogénnym skladom). Na prácu s cloudom sú potrebné aj pravidlá na riadenie aktívnych a frekventovaných dát. Ak sú podmienky splnené, môžeme hybridný cloud realizovať pomocou softvéru, gateways alebo integráciou aplikácií (Gsoedl, 2011).

Ako sme už uviedli, hybridný cloud je zložený z privátnych (min. 1) a verejných cloudov. Aby sme dosiahli heterogénny sklad, je potrebné, aby na interných a externých storage clouds bežal rovnaký softvér ukladania dát. Gateways slúžia na preklad protokolov, ale aj na prácu s rozhraním API. Prenos dát z jedného úložiska na druhé prebieha cez „policy engines". Brány sa od seba môžu líšiť optimalizáciou, návrhom, prípadne integráciou s aplikáciami. Implementácia pomocou integrácie aplikácií je založená na úložisku verejného cloudu cez rozhranie REST.

Bezpečnosť v cloude vychádza z jeho vlastnosti multi-tenancy. Dáta sú izolované od ostatných vrstiev a musia pokrývať bezpečnostné podmienky: utajenie, integrita, dostupnosť. Verejný cloud je prístupný väčšiemu počtu ľudí, a preto sa za hlavnú ochranu dát považuje kontrola prístupu. Ďalšou možnosťou je šifrovanie. Kryptografia zabezpečuje ochranu dát pomocou šifrovacích kľúčov, ktoré sa nachádzajú v najzákladnejšej vrstve – sieti. Zašifrovaným dátam treba priradiť autentizačné kódy. Dosiahneme tým druhú podmienku – integritu. Dostupnosť patrí k najkrehkejším podmienkam, nakoľko v prípade odstavenia elektrickej energie z dôvodu vonkajšieho faktora ju nemôžeme ovplyvniť. Čiastočné alebo dlhodobé obmedzenie dostupnosti môže spôsobiť čiastočnú, ale aj úplnú stratu dát. Pre verejný cloud je ukladanie aktívnych dát nevhodným riešením. Pri použití tohto riešenia si treba zvážiť bezpečnosť a výkon. Odolnosť a redundancia dát sa dosiahne tým, že sa každý objekt uloží na minimálne dva uzly.

Dosiaľ sme za najbezpečnejší považovali hybridný cloud. Podľa Sullivana (2012) vzhľadom na architektúru hybridného cloudu problém spočíva v prenose redundantných kópií dát. Ich presun cez dátové centrá pomocou virtuálnych strojov je jednoduchší ako medzi veľkými dátovými súbormi. Riešením by mohlo byť použitie viacerých dátových centier z jedného cloudu. Pri hybride je veľmi dôležité, aby boli verejné a súkromné cloudy kompatibilné. Pohyb medzi cloudami musí byť zabezpečený a treba dohliadať na miesta prenosu (metódy používané pri súkromnom cloude sa nemusia priamo prekladať do verejného cloudu). Hlavne pre hybridný cloud je charakteristické používanie nového rozhrania API a vyžadovanie komplexnej sieťovej konfigurácie. Nakoľko hybrid je zložitý systém a jeho administrátori majú limitované skúsenosti s riadením, vznikajú takto riziká. Ak chceme integrovať bezpečnostné protokoly, treba replikovať kontroly v oboch oblakoch. Zároveň treba udržiavať bezpečnostnú synchronizáciu dát. Druhou možnosťou je použitie správy identít služby, ktorá poskytuje jedinú službu pre systémy v oboch cloudoch.

Záver

Cloud computing je inovatívna technológia v IT, ktorá má svoje klady aj zápory. Zavedením cloudu sa vyriešili problémy s LAN, avšak vznikli nové otázky s bezpečnosťou uložených dát. Metódou označenia bezpečnosti pomocou troch parametrov (utajenie, integrita, dostupnosť) sme opísali možné riešenie. Cez architektúru a implementáciu sme bližšie pochopili funkcionalitu a riešenie modelov nasadenia cloud computingu – verejný, súkromný a hybridný model. Tretí model sa považuje za najbezpečnejší. Podľa najnovších výskumov treba pri tomto modeli riešiť päť základných problémov. Pri analýze opisu sme uviedli aj možné riešenia. V nasledujúcej tabuľke uvádzame výsledky našej analýzy troch modelov vzhľadom na ich použitie vo firme.

Vlastnosť	Verejný model	Súkromný model	Hybridný model
Počet klientov s prístupom do cloudu	+	–	+/–
Riadenie cloudu	–	+	+
Poskytovateľ	–	+	+/–
Spoľahlivosť	–	+	+/–
Nároky na implementáciu	–	-	+
Bezpečnostné podmienky	–	+/–	+/–

Odkazy

Gsoedl, J. (2011). Hybrid clouds: Three routes to implementation. Storage.

Rouse, M. (publikované jún 2009). TechTarget. Citované 21. augusta 2012. Dostupné na internete: http://searchcloudcomputing.techtarget.com/definition/private-cloud.

Rouse, M. (publikované máj 2009). TechTarget. Citované 21. augusta 2012. Dostupné na internete: http://searchcloudcomputing.techtarget.com/definition/public-cloud.

Rouse, M. (publikované jún 2010). TechTarget. Citované 20. augusta 2012. Dostupné na internete: http://searchcloudcomputing.techtarget.com/definition/hybrid-cloud.

Rybár, P. (publikované 14. apríla 2011). IT NEWS. Citované 23. augusta 2012. Dostupné na internete: IW: Cloud computing – quo vadis?: http://www.itnews.sk/tituly/infoware/2011-04-14/c139474-iw-cloud-computing-quo-vadis.

Sullivan, D. (publikované august 2012). TechTarget. Citované 25. augusta 2012. Dostupné na internete: Hybrid cloud: It's not as secure as you think: http://searchcloudcomputing.techtarget.com/tip/Hybrid-cloud-Its-not-as-secure-as-you-think.

Zuzana Priščáková

Mendelova univerzita v Brně
Provozně ekonomická fakulta