Bezpečnosť vo verejnom cloud computingu

■ PETER KIŠŠA

Koncept a implementácia architektúry cloudu sa môžu výrazne líšiť u jednotlivých poskytovateľov pre každý konkrétny model poskytovania služieb. Fyzické rozmiestnenie infraštruktúry, ako aj spôsob zabezpečenia jej spoľahlivosti a škálovateľnosti sú závislé od poskytovateľa, konkrétnej architektúry a použitých technológií.

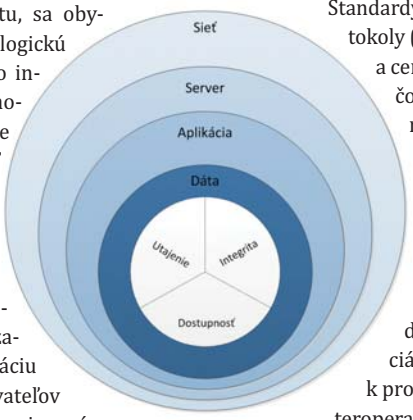
Architektonický princíp multi-tenancy umožňuje izoláciu dát a nastavení rôznych používateľov v rámci jednej zdieľanej infraštruktúry. Vysoká úroveň multi-tenancy na rôznych úrovniach architektúry celého cloudového systému je potrebná na to, aby sa dosiahla očakávaná flexibilita, spoľahlivosť a nákladová efektivita. Na splnenie spomenutých požiadaviek musí poskytovateľ zabezpečiť vysoko dynamické a flexibilné poskytovanie služieb a súčasne bezpečnú izoláciu zdrojov používateľov.

Technológia virtualizácie je softvérová vrstva medzi operačným systémom a hardvérom, ktorá umožňuje poskytovateľom cloudových služieb IaaS operovať vysoko efektívnu platformu multi-tenancy. Virtualizácia okrem virtualizovaných prostriedkov poskytuje aj služby na ich správu, kde pomocou vlastného aplikačného rozhrania umožňuje vykonávať administratívne úkony, ako je spúšťanie, migrovanie a terminovanie virtuálnych prostriedkov. Rozhranie na manažment zväčšuje priestor na potenciálny útok a tým prispieva k zvýšeniu bezpečnostného rizika.

Virtuálne prostriedky takisto ako klasické musia byť adekvátne zabezpečené fyzicky aj logicky. V rámci interných postupov a politík organizácie treba dôsledne zabezpečiť operačné systémy a nasadené aplikácie pred finálnym vytváraním produkčného obrazu (image) virtuálneho stroja. Je dôležité venovať zvýšenú pozornosť správe týchto virtuálnych obrazov, aby sa napríklad zabránilo nasadeniu nezabezpečeného obrazu, využívaného na vývoj, omylom na produkčné prostredie.

Vedľajším efektom virtualizovaných prostredí je riziko potenciálnej straty logickej kontroly pre separáciu povinností (separation of duties) v rámci existujúcich administratívnych rolí v organizácii. V rámci virtualizovanej infraštruktúry sa často dištinktívne administratívne roly zlúčia do jednej ako dôsledok zjednoteného grafického rozhrania konzoly manažmentu. Kompenzáciou tohto problému môže byť zavedenie dodatočných interných mechanizmov kontroly v organizácii.

Realizácia konceptu multi-tenancy pre služby PaaS a SaaS, potrebného pre očakávanú cloudovú efektivitu, sa obyčajne spolieha na jednu logickú inštanciu aplikácie. Táto inštancia je schopná pomocou up-scale a down-scale dynamicky sa adaptovať podľa potreby a potenciálne tak obslúžiť aj veľké množstvo používateľov. Bez ohľadu na konkrétne použitú architektúru musí realizácia zabezpečiť dostatočnú izoláciu jednotlivých používateľov služby tak na dátovej, ako aj na výpočtovej úrovni.



Obr. 1

Bezpečnosť a ochrana dát

Dáta uložené v rámci infraštruktúry verejného cloudu sú obyčajne umiestnené v zdieľanom prostredí a kolokované s dátami ostatných používateľov. Organizácia, ktorá sa rozhodne umiestniť senzitívne informácie do takejto zdieľanej infraštruktúry, preto musí zodpovedať za to, ako je kontrolovaný prístup k jej dátam a ich celkové zabezpečenie.

S dátami uloženými vo verejnom cloude sú rovnako, ako keby boli uložené hocikde inde, spojené tri základné princípy v oblasti bezpečnosti informácií: utajenie, integrita a dostupnosť (Confidentiality, Integrity, Availability). Navyše informácia v kontexte týchto princípov musí byť zabezpečená na všetkých úrovniach systému, či už je v pokoji, v tranzite, alebo používaná službou.

Utajenie dát

Zabránenie neoprávnenému prístupu k informáciám v cloude je jedna z kľúčových úloh efektívnej ochrany dát. Problém je v tom, že existujúce mechanizmy autentifikácie a autorizácie v rámci organizácie sa obyčajne nedajú jednoducho aplikovať na cloudové služby. Používanie dvoch separátnych autentifikačných mechanizmov, jedného pre interné systémy a služby a druhého pre externé cloudové služby, je komplikácia, ktorá sa môže stať časom aj principiálne nefunkčnou. Federatívny manažment identít a autentifikácia je mechanizmus, ktorý organizácii umožní zdieľanie digitálnych identít medzi internými a externými cloudovými službami a v konečnom dôsledku umožní využitie Single Sign-On.

Dáta môžu mať mnoho podôb: aplikačné programy, skripty, konfiguračné nastavenia, dátové záznamy, ako aj informácie o používateľoch a ich nastavení. Ochranu údajov pred neoprávnenými používateľmi možno zabezpečiť dvoma spôsobmi, a to kontrolou prístupu a ich šifrovaním.

Štandardy pre komunikačné protokoly (obr. 1 – sieťová úroveň) a certifikáty šifrovacích kľúčov umožňujú zabezpečenie dátových tokov pomocou kryptografie. Postupy na ochranu dát v pokoji (obr. 1 – úroveň servera) sú takisto bežne dostupné, i keď nie sú zvlášť štandardizované, čo potenciálne môže viesť k problémom spojených s interoperabilitou. Práca nad zašifrovanými informáciami (obr. 1 – úroveň aplikácie) je síce aktuálne veľmi dynamická oblasť, na ktorú sa sústreďuje výskum, ale zatiaľ bez väčších praktických výsledkov.

Ďalší proces v rámci opatrení na ochranu informácií na strane poskytovateľa služieb je dôkladné mazanie už nepotrebných dát. Ide o vymazávanie dát z pamäťových médií prepísaním, odmagnetizovaním alebo inými prostriedkami (napr. fyzické zničenie médií) tak, aby sa zabránilo nepovolenému zverejneniu informácií tretím stranám. Toto zahŕňa rôzne údržbové a prevádzkové scenáre, keď sa pamäťové médiá v rámci ich životného cyklu znova nasadzujú alebo vyraďujú z prevádzky. Mazanie dát sa vzťahuje aj na automaticky vygenerované záložné kópie na obnovu služieb, ako aj zvyškové dáta zostávajúce po terminácii služby.

Integrita dát

Okrem úrovne a kvality utajenia dát v cloude je ďalší dôležitý princíp zachovanie integrity dát. Samo utajenie nezaručuje zachovanie integrity: dáta síce môžu byť zašifrované, ale organizácia nemusí mať spôsob verifikácie integrity dát. Dáta v zašifrovanej podobe spĺňajú princíp utajenia, ale integrita dát vyžaduje navyše ešte použitie autentizačných kódov (message authentication code – MAC).

Táto úloha je ešte ťažšia pri verejnom cloude, pretože organizácia nemôže vedieť,

na akých konkrétnych fyzických zariadeniach je daná informácia uložená. Okrem toho, že dáta sú dynamické a často sa menia, prenos dát z cloudovej infraštruktúry a do nej má aj svoje náklady, a tak sa musí vo väčšine prípadov spoliehať na existujúce mechanizmy na strane poskytovateľa.

Dostupnosť dát

Posledný princíp bezpečnosti informácií, ktorý treba dodržiavať a kontrolovať, je princíp dostupnosti. Jednoducho povedané, dostupnosť definuje mieru prístupnosti a použiteľnosti výpočtových zdrojov a dát organizáciou. Dostupnosť môže byť ovplyvnená dočasne alebo trvalo a strata môže byť čiastočná alebo úplná. Problém je, že odstávky sú väčšinou neplánované a môžu mať priamy vplyv na chod organizácie.

Existuje určitá pravdepodobnosť, že poskytovateľ cloudových služieb narazí na vážne problémy (výpadky zdrojov v prípadoch prírodnej katastrofy a pod.), ktoré môžu ovplyvniť dostupnosť služieb na dlhší čas. Pravdepodobnosť je však pre organizáciu prinajmenšom rovnaká, a tak by mala kriticky zvážiť svoju vlastnú pripravenosť a schopnosť riešiť takéto problémy (záložné generátory, duplicitné sieťové linky a pod.). Každopádne, ak organizácia používa cloudové služby a spolieha sa na ich dostupnosť, mala by mať krízový plán pre prípady výpadkov týchto služieb.

Schopnosť poskytovateľa cloudových služieb dynamicky škálovať obranné prostriedky a mechanizmy na požiadanie má zjavné výhody pre bezpečnosť, odolnosť a dostupnosť poskytovaných služieb. Keď je táto schopnosť dynamického škálovania skombinovaná s vhodnými metódami optimalizácie zdrojov, poskytovateľ môže efektívne minimalizovať dosahy bezpečnostných rizík, a to s nižšími konečnými nákladmi.

Autor pracuje ako softvérový analytik a cloudový špecialista v spoločnosti InterWay, s.r.o.