Správa používateľov v oblakoch

Služby označované ako cloud sú v poslednom čase extrémne populárne. A niet sa čomu čudovať. Väčšina zložitosti týchto služieb je úspešne skrytá na strane ich poskytovateľa. A jednoduchosť, ktorú tieto služby prezentujú používateľom, je obzvlášť atraktívna.

Oblaky služieb prinášajú zákazníkom ponuky, ktoré sa často zdajú lacnejšie a flexibilnejšie ako ekvivalentné služby poskytované interným IT personálom. Niektoré ponuky sú až pridobré na to, aby boli pravdivé. Ako to už často býva, ani pri cloudových službách nie je všetko také jednoduché, ako to na prvý pohľad vyzerá.

Tieto internetové služby majú väčšinou veľmi jednoduchú registráciu používateľov a dokonca neraz poskytujú časť funkcionality zadarmo. Toto zamestnanci radi využívajú a sami si vytvárajú používateľské účty. Tie sa postupne plnia firemnými údajmi, ktoré majú nezriedka citlivý charakter. Keďže si zamestnanec založil účet sám, tento účet nie je pod kontrolou firmy. Bezpečnostné oddelenie firmy má len malý prehľad o tom, kde a ako sú údaje uložené, čo je samo osebe závažný bezpečnostný problém. Veľké ťažkosti však nastávajú pri odchode zamestnanca. Zamestnanec si po odchode takto založený účet väčšinou necháva. A spolu s účtom si necháva aj dáta uložené na ňom. Nekontrolované využívanie cloudových služieb je kritické bezpečnostné riziko pre takmer každú organizáciu.

Preto jedna z oblastí, ktorá sa dotkne používateľov cloudových služieb hneď ako prvá, je správa používateľov. Z bezpečnostného hľadiska je väčšinou úplne neprijateľné, aby si zamestnanec vytváral a spravoval účet sám. Preto sa jeho účet musí vytvoriť (a najmä zrušiť) v presne definovanom a dobre riadenom procese správy identít. Tento proces už v takej či onakej podobe v každej firme existuje. Vo väčšine prípadov je však manuálny. A tu vstupuje do hry ďalší zaujímavý aspekt cloudových služieb: sú väčšinou jednoúčelové a relatívne lacné. Preto je reálne očakávať, že firma bude využívať viac cloudových služieb, ako bol počet tradičných aplikácií. Očakávaný počet využívaných služieb veľmi rýchlo prekročí možnosti manuálneho procesu správy identít a automatizácia sa stane nevyhnutnou.

Automatizáciou procesov správy identít sa zaoberá oblasť nazývaná správa identít a prístupov (Identity and Access Management, IAM). Nasadenie automatizovaného riešenia IAM je dnes už nevyhnutnosť pre každú strednú a väčšiu organizáciu. Lenže cloud aj túto oblasť mierne mení. A to nás privádza k ďalšiemu závažnému problému.

Služby poskytované ako cloud nie sú technologicky prevratné oproti ich tradičným ekvivalentom. Prevádzkovatelia cloudových služieb sa spoliehajú na prínosy z masívnej ekonomickej škálovateľnosti. Prevádzkovateľ takejto služby musí poskytnúť tú istú službu obrovskému počtu používateľov, aby ju mohol ponúkať lacnejšie, kvalitnejšie a ešte aj vykázal dostatočný zisk. To však znamená, že služba už nemôže byť prispôsobená presne potrebám každého jedného zákazníka. Práve naopak. Zákazník sa musí prispôsobiť službe. Každej jednej službe osobitne. To, čo cloud získava na jednoduchosti použitia, veľmi často stráca v integračnej oblasti.

Keďže cloud už nie je interný systém, bežné prístupy sa takmer nedajú použiť. Firemný bezpečnostný perimeter je definitívne zavrhnutý do minulosti. Centrálna zdieľaná adresárová služba (LDAP), dátové pumpy a podobné jednoduché mechanizmy v týchto prípadoch nie sú postačujúce. Každý cloudový systém poskytuje vlastné rozhranie na správu používateľov. Každé z nich je úplne iné a mnohé sú žalostne nedostatočné. Preto sa riešenie IAM musí prácne prispôsobovať každej cloudovej aplikácii osobitne. Jediné praktické východisko z tejto situácie je použitie riešenia IAM, ktoré sa prispôsobuje relatívne ľahko a lacno. V opačnom prípade integračná snaha môže veľmi jednoducho anulovať všetky výhody využitia cloudových služieb. Zrejme by pomohla štandardizácia rozhraní IAM. A v oblasti riadenia prístupov a jednotného prihlásenia je situácia relatívne priaznivá. Veľký problém je však štandardizácia v oblasti správy identít (provisioning). V tejto oblasti už niekoľko pokusov o štandardizáciu zlyhalo (napr. SPML). Najnovší pokus, nazývaný SCIM, vynucuje schému, ktorá je veľmi málo kompatibilná s väčšinou existujúcich systémov. Aj preto je málo pravdepodobné, že by tento štandard uspel.

Ani úspešný štandard, nech je akýkoľvek nepravdepodobný, však problém úplne nerieši. Ak sa aj podarí preniesť väčšinu zodpovednosti za bezpečnosť dát na poskytovateľa cloudovej služby, ani jeden rozumný poskytovateľ neprevezme záruku za únik dát z platného účtu. Preto je za akýchkoľvek okolností potrebný dobrý, prispôsobiteľný a spoľahlivý systém IAM. Takýto systém sa musí postarať o to, aby sa účty včas deaktivovali a nebola tým porušená dátová bezpečnosť.

Žiaľ, tradičné podnikové riešenia IAM majú často korene ešte v 20. storočí a pre prostredie internetu nie sú vôbec ideálne. Kombinácia zastaraných technológií a vysokej ceny ich z použitia v prostredí cloudových služieb takmer úplne diskvalifikuje. Našťastie v posledných rokoch sa začínajú objavovať riešenia IAM druhej generácie. Tieto produkty sú oveľa modernejšie, flexibilnejšie a podstatne lacnejšie. Nová generácia produktov vznikla od základu v internetovom veku, a preto aj integráciu na cloud zvláda dostatočne dobre. Tieto produkty sú už dosť vyzreté a známe, takže kvalifikovaný odborník by nemal mať problém navrhnúť vhodné, komplexné a pritom finančne nenáročné riešenie.

Aj napriek spomenutým problémom sú cloudové služby veľmi užitočné a atraktívne. Treba však pamätať na to, že ani pri využívaní týchto „vzdušných" alternatív nemožno zanedbávať správnu podnikovú architektúru a infraštruktúru. Riešenie správy identít je jeden z najdôležitejších aspektov využívania cloudových služieb. Preto prv ako začnete intenzívne využívať služby v oblakoch, choďte sa poradiť k svojmu podnikovému architektovi alebo systémovému integrátorovi, ako to robiť efektívne a bezpečne.

RADOVAN SEMANČÍK
Software architect,
radovan.semancik@evolveum.com
Evolveum, s. r. o.