Správa identít a prístupov v internete

» Internetové a podnikové prostredie sa v poslednom desaťročí podstatne priblížili. Dnes už nie je nezvyčajné vidieť internetové technológie, ktoré sú základnými stavebnými prvkami podnikových technológií. A naopak, internetové technológie sa približujú požiadavkám podnikových informačných systémov najmä v oblasti bezpečnosti a spoľahlivosti. Ale aj napriek tomuto približovaniu majú jednotlivé prostredia svoje špecifiká. V správe identít a prístupov je tento rozdiel podstatný. Je to zrejme dané veľkými odlišnosťami v základných črtách jednotlivých prostredí. Kým v podnikovom prostredí sa spravujú uzatvorené skupiny používateľov (najmä zamestnanci), v internetovom prostredí je skupina používateľov otvorená a takmer nekontrolovateľná. Ďalší dôležitý rozdiel je vo veľkosti. Pre podnikové prostredie sú typické tisíce až státisíce identít. Riešenie pre internetové prostredie musí počítať s množstvami používateľov, ktoré sú o niekoľko rádov vyššie. Preto technológie na správu identít a prístupov (Identity and Access Management, IAM) v internetovom prostredí majú svoje neprehliadnuteľné špecifiká.

Je zrejmé, že prakticky nemožno vytvoriť jednu centrálnu databázu všetkých používateľov internetu. O niečo podobné sa pred niekoľkými dekádami snažila technológia X.500. Aj keď niektoré jej časti žijú doteraz, pokus o vytvorenie jednej celistvej databázy X.500 neuspel. A zrejme ani uspieť nemohol, pretože internet je zložený z množstva veľmi nesúrodých systémov, ktoré je týmto spôsobom takmer nemožné integrovať. Preto sa pre prostredie internetu momentálne presadzuje úplne iný prístup, založený na koncepte federácie.

Pri použití federácie identít má každý zapojený internetový uzol svoj vlastnú databázu používateľov. Táto databáza sa využíva na autentifikáciu používateľov, ktorí patria k tomuto uzlu, napríklad zamestnancov firmy alebo študentov univerzity. Keď takýto používateľ pristupuje k inému federovanému uzlu, informácia o jeho identite sa prenesie na tento uzol pomocou dohodnutých komunikačných protokolov. Vzdialený uzol potom môže vidieť vybrané aspekty identity používateľa. Tento prístup sa veľmi často používa v akademickom prostredí, kde je takmer nevyhnutný na efektívnu spoluprácu medzi univerzitami. Napríklad študent univerzity A sa prihlási vo svojom univerzitnom systéme pomocou svojho mena a hesla. Tento študent sa rozhodne pristúpiť k elektronickým zdrojom v knižnici univerzity B. Pomocou protokolov federácie identít sa knižničný systém dozvie, že komunikuje so študentom univerzity A a na základe toho mu povolí prístup. Univerzita A v tomto prípade vystupuje ako poskytovateľ identity (identity provider), knižnica vystupuje ako poskytovateľ služby (service provider).

Zaujímavý aspekt tohto prístupu je zachovanie bezpečnosti a súkromia používateľov. Knižnica ako poskytovateľ služby vie len minimum informácií, ktoré potrebuje. Knižnica nevidí heslo používateľa, keďže používateľ sa autentifikuje len vo svojej domovskej univerzite. Knižnica vie, že ten, kto pristupuje, je denný študent univerzity A. To je všetko, čo knižnica potrebuje vedieť na poskytnutie prístupu. Knižnica sa nedozvie meno študenta, jeho číslo ani žiadny iný dôležitý identifikátor. Podobne to platí aj v opačnom smere: univerzita vie, že študent pristúpil do knižnice, ale už nevie, k akým konkrétnym zdrojom pristupoval. Takýto federatívny prístup v rozumnej miere zachováva súkromie. používateľov.

Tento prístup bol navrhovaný primárne pre plne distribuované prostredie, kde sa predpokladala prítomnosť veľkého množstva poskytovateľov identít. Je pri ňom zachovaná bezpečnosť systému, ako aj akceptovateľné súkromie používateľov. V tejto forme sa federácia identít používa na medzinárodnú spoluprácu v akademických sieťach. Komerčná sféra však tento prístup pozmenila. V komerčnej oblasti sú poskytovateľmi identít väčšinou len internetové megakorporácie. Tým sa redukuje počet poskytovateľov identít na niekoľko obrovských firiem. Aj pri použití bezpečných technológií sa však poskytovateľ identity dozvie o používateľovi isté informácie, napríklad systémy, do ktorých pristupoval. Preto systém, v ktorom je niekoľko gigantických poskytovateľov identity, predstavuje veľké riziko. Každý poskytovateľ identity vie čiastočne profilovať obrovské množstvo používateľov. Pri tomto prístupe súkromie používateľov trpí.

Z technologického hľadiska internetovým systémom na správu identít a prístupov dominujú najmä dve rodiny protokolov SAML a OAuth. SAML je služobne starší a vyzretejší protokol. Je založený na XML a je relatívne komplikovaný. Poskytuje však pokročilé funkcie a je schopný prevádzkovať aj veľmi rozsiahle federácie. Používa sa najmä v akademickom prostredí, rozsiahlych podnikových partnerských sieťach a v programoch na eGovernment.

OAuth je služobne mladší protokol a je primárne navrhnutý pre prácu v prostredí RESTful. OAuth je zdanlivo jednoduchší protokol. Jeho jednoduchosť je však čiastočne daná faktom, že špecifikácia OAuth nedefinuje konkrétny protokol, ale obsahuje len relatívne vágne odporúčania, ako protokol zostrojiť. Preto OAuth je prakticky použiteľný len tak, že každá implementácia si tieto medzery v definícii doplní svojím spôsobom. Je však pravdepodobné, že každé nasadenie OAuth bude mierne iné, a preto interoperabilita implementácií OAuth je obrovský problém. Snažia sa ho riešiť dve špecifikácie: OpenID Connect a User-Managed Access (UMA). OpenID Connect špecifikuje služby na distribuovanú autentifikáciu používateľa a prístup k jeho používateľskému profilu. UMA rieši distribuovanú autorizáciu na prístup k internetovým zdrojom.

Obe špecifikácie sú však relatívne mladé a stále nie sú dostatočne ustálené. OAuth a jeho deriváty sa začínajú používať na riadenie prístupu k službám RESTful v uzatvorených podnikových systémoch. V takýchto prípadoch je OAuth veľmi prospešný, keďže pre prostredie RESTful iný praktický spôsob takmer neexistuje. V uzatvorených prostrediach sú problémy s interoperabilitou implementácií OAuth nepríjemné, ale väčšinou riešiteľné. Inak je to však v prostredí internetu. Tu sa používa takmer výlučne OpenID Connect a jeho modifikované verzie, ktoré si internetové megakorporácie upravili pre svoje potreby. Interoperabilita implementácií je relatívne nízka, a preto treba implementácie prispôsobovať pre každého poskytovateľa identít osobitne.

Aj keď sa technológie na internetovú správu identít objavili pred viac ako dekádou, ich schopnosti a nasadenia sú stále len na začiatku. Tieto technológie majú často veľké problémy so zachovaním súkromia, pokročilou správou prístupov (zložitejšie privilégia), ale napríklad aj s dlhodobou konzistenciou údajov. Hoci sú tieto technológie v niektorých prípadoch prakticky použiteľné, ich limitácie sú veľmi závažné. Neodporúčame ich používať bez predchádzajúcej prípravy. Konzultácie so skúseným odborníkom sú v tomto prípade viac ako potrebné.

» RADOVAN **SEMANCIK**
Software architect, EVOLVEUM