Riadenie prístupov

Správa identít a prístupov (Identity and Access Management, IAM) je relatívne široká oblasť, zložená z množstva spolupracujúcich technológií.

Jedna z nich však silne vystupuje do popredia: riadenie prístupov (*Access Management*, AM). Nie je to preto, že by bola dôležitejšia ako iné. Ale na rozdiel od ostatných technológií IAM, ktoré si pokojne žijú niekde v pozadí informačnej infraštruktúry, technológie riadenia prístupu vstupujú používateľovi priamo do cesty. Do tejto skupiny patria najmä technológie jednotného prihlasovania (Single Sign-On, SSO) a čiastočne aj rôzne autentifikačné a autorizačné technológie. Preto ak sa nemôžete prihlásiť do informačného systému, zrejme za to môže nejaký z komponentov, o ktorých píšeme v tomto článku.

V tradičných aplikáciách autentifikáciu, autorizáciu a podobné bezpečnostné mechanizmy implementuje každá aplikácia osobitne. Tento prístup je zjavným plytvaním zdrojmi, keďže prevádzkovateľ musí platiť za tú istú funkcionalitu niekoľkokrát, a to nielen za jej vývoj, ale aj za jej konfiguráciu a prevádzku. Navyše jednotlivé aplikácie o sebe navzájom nevedia a používateľ sa musí prihlásiť do každej aplikácie znova a znova. A práve riešením týchto problémov sa zaoberajú technológie správy prístupov.

Zjednodušene by sa dalo povedať, že základný princíp riadenia prístupov je oddelenie autentifikácie používateľa od aplikácií. Prihlásenie (autentifikáciu) používateľa v tomto prípade zabezpečuje centralizovaný komponent, väčšinou označovaný ako SSO alebo AM server. Ten zabezpečí, aby používateľ nemusel zadávať svoje prihlasovacie údaje pre každú aplikáciu zvlášť, ale len pri prvom prístupe k niektorej z integrovaných aplikácií.

Proces jednotného prihlásenia zabezpečovaný centrálnym autentifikačným serverom by sa stručne dal opísať takto. V prípade prvého prístupu k aplikácii je používateľ presmerovaný na SSO server, kde sa pomocou svojich prihlasovacích údajov autentifikuje. Po úspešnom prihlásení je presmerovaný naspäť na aplikáciu spolu s „tokenom" obsahujúcim informácie o prihlásenom používateľovi. V prípade, že sa tento používateľ rozhodne pristúpiť k inej aplikácii, je znova presmerovaný na SSO server. No ten už vie, že používateľ bol autentifikovaný, a okamžite ho presmeruje späť na aplikáciu, ktorá mu na základe existujúceho „tokenu" umožní prístup. Kým sa používateľ neodhlási z niektorej aplikácie alebo neprekročí definovaný čas nečinnosti, môže pracovať s aplikáciami bez nutnosti opätovného prihlásenia.

Čiastočne môže SSO server zabezpečiť aj autorizáciu. Granularita autorizácie je väčšinou len na úrovni povolenia/zamietnutia prístupu úspešne autentifikovaného používateľa k danej aplikácii. O jemnejšej granularite autorizácií, ako je napríklad oprávnenie vykonávať konkrétnu akciu alebo možnosť zobraziť určitý prvok v menu, už rozhoduje každá aplikácia samostatne.

Tento jednoduchý princíp má svoje výhody. Medzi najvýraznejšie z nich patrí flexibilita. Predstavme si, že sa zmenia bezpečnostné požiadavky na autentifikáciu. Kým v prípade klasického riešenia treba upravovať každú aplikáciu zvlášť, pri využití jednotného prihlásenia stačí zmeniť spôsob autentifikácie na strane SSO servera. Navyše SSO server môže vyhodnotiť, odkiaľ a v akom čase používateľ pristupuje, porovnať to s predchádzajúcimi prístupmi a vynútiť silnejšiu autentifikáciu, ak sa jeho zvyky zrazu zmenia. Či už ide o zmenu bezpečnostnej politiky, globálnej autorizácie, alebo je potrebná implementácia dvojfaktorovej autentifikácie, to všetko sa dá dosiahnuť len zmenou SSO servera bez zásahu do aplikácií.

Z dlhodobého hľadiska správa prístupov šetrí nemalé prostriedky, no napriek tomu netreba zabúdať, že aj to má svoju cenu. Menšiu časť celkovej ceny projektu predstavuje nasadenie a prispôsobenie SSO servera, tú väčšiu integrácia jednotlivých aplikácií. Aplikácie, ktoré majú byť súčasťou riešenia, treba prispôsobiť, a to modifikovať alebo prekonfigurovať ich natívny autentifikačný mechanizmus. Cena týchto modifikácií, potrebného testovania, ako aj organizačné náklady často niekoľkonásobne prevýšia cenu SSO servera.

Pri nasadzovaní systémov riadenia prístupu je tu však jeden kritický moment, a to potreba spoľahlivej centrálnej databázy používateľov. Táto požiadavka sa zdá triviálna, ale vo väčšine prípadov je to obrovský problém. Napriek tomu, že množstvo aplikácií umožňuje jednoduché pripojenie na systémy riadenia prístupov, neraz používajú svoje databázy používateľov a napríklad veľmi často používajú rôzne identifikátory pre rovnakých používateľov. Preto je nepravdepodobné, že by bolo možné nasadiť technológie riadenia prístupu priamo na existujúci informačný systém bez predchádzajúcej prípravy.

Nasadenie systému na riadenie prístupu preto predchádza nasadenie systému na správu identít (IDM). Systém IDM sa využije práve na unifikáciu databáz používateľov jednotlivých aplikácií a vytvorenie centrálnej databázy, väčšinou reprezentovanej adresárovým systémom. Po „upratání" identít potom možno nasadiť systém na správu prístupov.

Produktov na riadenie prístupov je veľké množstvo. Sú tu nákladné komerčné produkty, dostupné produkty s otvoreným zdrojovým kódom, jednoduché aj prekomplikované produkty a takmer každý zákazník si nájde to svoje. Problémom je však ich vzájomná kompatibilita , a preto treba vyberať produkt veľmi zodpovedne. V neposlednom rade je rovnako dôležité uvedomiť si celkové náklady nasadenia systému na správu prístupov. Ako už bolo spomínané, tie sa viažu hlavne na poznanie súčasného stavu, potrebu unifikácie databáz jednotlivých aplikácií, potrebu vytvorenia centrálnej databázy a potrebu prispôsobiť autentifikačné mechanizmy pripájaných aplikácií.

Technológie riadenia prístupu sú povestnou špičkou ľadovca v riešeniach IAM. Jednotné prihlásenie, centrálne vynucovanie autentifikačných politík a ďalšie vlastnosti týchto technológií sú to, čo bežný človek (nie úplne správne) vníma pod pojmom správa identít. Aby táto špička ľadovca dokázala efektívne plniť svoj účel, sú nevyhnutné aj ďalšie technológie, ktoré sú skryté pod hladinou vnímania bežného človeka. Preto na efektívnu implementáciu týchto technológií je vhodné požiadať o pomoc skúseného odborníka so širokým prehľadom v celej oblasti IAM.

» KATARÍNA **VALALIKOVÁ**
Software developer,
k.valalikova@evolveum.com

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