

Manažment rolí v riešeních identity

Pri návrhu riešenia Identity & Access Management (IAM) u zákazníka som narazil na vážny problém. Bolo ním postavenie koncepcie rolí používateľov riadených produktom identity management (IDM), ich optimalizácia a progresívne pridelovanie. Určite každý architekt riešenia IDM sa s tým stretáva pri návrhu a zákazník, ktorý nasadzuje riešenie IDM, sa snaží pochopiť, prečo správne definovanie rolí v riešeních identity má kľúčový význam pre jeho projekt. Ak teda nasadenie IDM je strategickým rozhodnutím firmy, správa rolí a koncepcia ich tvorby a manažmentu je strategickým rozhodnutím architektov a administrátorov riešenia identity.

Čo sú roly používateľov IS v riešení IDM

Vo všeobecnosti možno povedať, že ide o biznis pohľad na kumulované práva používateľa informačných systémov spoločnosti. Roly v riešení identity zastrešujú viacero nastavení a práv, ktoré sú držiteľovi roly automatizovane pridelované identity managerom tak, že vytvárajú medzi entitou rola v riešení identity a kapabilita na koncovom systéme vzťah 1 to N. Tento model zabezpečuje ďalej optimalizáciu správy používateľov, ako aj optimalizáciu procesov žiadania o pridelenie prístupových práv prostredníctvom riešenia identity.

Stratégia zavádzania rolí

V návrhu riešenia identity je tvorba návrhu rolí súčasťou analytického dokumentu, ktorý vzniká pred nasadením riešenia identity a ďalej sa optimalizuje v časti User management projektu. Z koncepčného hľadiska pri zavádzaní konceptu rolí treba klásť veľa otázok. Pýtať sa správcov koncových systémov, akým spôsobom je zabezpečená správa používateľov, pýtať sa pracovníkov HR, ako nadväzuje pracovná pozícia na práva v IS, pýtať sa manažmentu, ako si predstavuje schvaľovací model žiadania o prístupové práva a podobne. Správca informačného systému prideluje práva používateľovi v dvoch základných koncepciách: per User alebo per Group. Zväčša je koncepčne správny druhý prípad a rovnako, ako správcovia koncových systémov kumulovali tieto práva, roly IDM túto funkciu vykonávajú naprieč viacerými koncovými systémami. Najjednoduchší spôsob je vytvoriť taký

počet rolí, aký je počet skupín v koncových systémoch. Rýchle a azda aj rozumné. Ale z pohľadu správcu systému IDM a jeho používateľov ide o cestu do pekla IDM. Používanie takýchto rolí sa stáva neprehľadným a ťažkopádny.

Ako postupovať pri zavádzaní rolí

Model IAM maturity, ako spôsob prehodnotenia vyspelosti aktuálneho a želaného stavu riešenia IAM, automatizovanú správu rolí zaraďuje ako znak štandardizovaného stavu obchodného procesu. Súčasné riešenia identity priamo ponúkajú vytváranie hierarchických modelov rolí či biznis rolí. Existuje veľa teoretických postupov, ktoré radia, ako prepojiť používateľské práva a priradené roly. Model Role Based Access (RBAC), t. j. prístup používateľa na základe pridelených rolí, je známy už veľmi dlho. Koncepčne sa ako správny postup osvedčila tvorba stavových tabuliek prístupov do koncových systémov, pričom na základe jej analýzy možno vytvoriť kumulované biznis roly. Tie možno ešte ďalej optimalizovať a vytvárať tlak na definovanie a optimalizáciu biznis modelov spoločnosti. Problémom však stále zostane ich modulácia v čase, keďže aj informačné systémy spoločnosti sa menia, analýza rolí zostáva trvalým procesom. Prvotný zoznam rolí sa rozširuje, dopĺňa a mení, pričom táto úloha zväčša zostáva na pleciach administrátorov IDM. Vynára sa otázka, ako a či vôbec tento proces možno vykonávať štandardizovanými prostriedkami tak, aby ponúkal komfortné rozhranie, analytickú presnosť a podporu od dodávateľa.

Role Management

Rovnakú otázku si kladli i dodávatelia a producenti riešení IDM, a keďže potreba trhu robí niečo lepšie tvorí základ pre správny obchodný zámer, vznikli produkty Role Management. Tieto produkty zabezpečujú nielen tvorbu rolí, ale aj správu ich životného cyklu. Dnes už každý veľký výrobca ponúka Role Management ako súčasť svojho portfólia IDM. Ako si však vybrať tie správne nástroje na Role Management? Je to často skôr otázka pocitov, keďže funkcionality produktov technologických špičiek je takmer totožná. Zväčša sa postupuje podľa

hesla: Aké riešenie IDM máš, také riešenie Role Management si doplníš.

Problémom týchto riešení však zostáva vyššia logika systému tvorby rolí. Čo si pod týmto pojmom možno predstaviť? Je pochopiteľné, že práva používateľov sa často modulujú nielen v závislosti od toho, aké povinnosti majú, ale aj kde ich vykonávajú, či sú ich povinnosti podmienené dočasnou úlohou, či prístupujú do systémov zvnútra firmy, či môžu niektoré činnosti vykonávať i doma a podobne. Všetky tieto faktory a ich kombinácia majú modulovať aj systém rolí, čo však nie je také jednoduché. Nejde o statický proces a vytvorenie sofistikovaných modelov, ktoré možno zapracovať do IDM, je často problematické. Ako optimálny postup sa osvedčilo využitie protokolu SPML ako medzichánku medzi modulom dynamickej správy identít a systémom IDM. Na slovenskom trhu je v tejto doméne už 10 rokov etablovaný produkt, ktorý dynamický spôsob pridelovania rolí využíva. Jeho funkcionality je založená práve na matematických modeloch, ktoré modulujú roly pridelené používateľovi, pričom jeho funkčnosť v riešení IDM možno využiť tak prostredníctvom SPML, ako aj webových služieb. Prepojením riešenia identity managementu, role managementu a systému dynamických rolí administrátor dostáva jedinečnú komplexnú kombináciu nástrojov, ktoré mu umožnia efektívnu správu životného cyklu používateľa.

Čo dodať na záver?

Správa životného cyklu rolí používateľa je dynamický proces. Koncipovanie modelu rolí, prvotná analýza bez využitia optimalizačných nástrojov, ako je Role Manager, sú veľmi problematické a zväčša čas, ktorý sme relatívne ušetrili preberaním rolí z koncových systémov, sa niekoľkonásobne negatívne prejaví pri správe a výkone systému. Z tohto dôvodu treba klásť veľký dôraz na inicializáciu projektu. Výsledky tvorby a manažmentu rolí by však nemali zostať iba súčasťou riešenia identity. Je potrebná prepojenosť s procesným modelom riadenia organizácie a takto vytvorený model nástroja IT a podnikových pravidiel vytvorí synergiu riadenia.



■ RADOSLAV HUDEC, produktový manažér Identity & Access Management PosAm, spol. s r. o.

PosAm

USEFUL
TECHNOLOGIES

need+identity+management+useful

PosAm Identity & Access Management^{UT}
www.posam.sk