

Správa identit s využitím adresářových služeb

IT System (březen 2005)

Úměrně tomu, jak informační technologie pronikají do mnoha oblastí lidské činnosti, narůstá počet uživatelů, kteří s nimi pracují. Ve středních a velkých firmách se každý den stovky či tisíce zaměstnanců přihlašují k desítkám firemních aplikací i k systémům neustále vzrůstajícího počtu obchodních partnerů. Stále více zákazníků navštěvuje nové firemní portály. Mase těchto uživatelů je třeba zpřístupnit zdroje, jež potřebují využívat. K tomu je vhodné použít správného systému správy identit, který firmě může ušetřit peníze, zajistit spokojenější uživatele a zlepšit bezpečnost IT.

Během rozšiřování množiny systémů a uživatelů se postupně objevují následující problémy:

- pro koncové uživatele je poměrně dost komplikované nalézt požadované služby a zdroje a dozvědět se o nových, které v dané síti existují
- pro aplikace je naopak obtížné sdílet informace o službách, zdrojích a uživateli, protože jsou často uloženy v aplikačně závislých databázích
- se vzrůstajícím počtem služeb narůstá i množství správy, které navíc komplikuje hledisko složitosti propojení systémů, které nejsou platformně závislé
- a jedním z neposledních bodů, je otázka řízení bezpečnosti v jednotlivých částech sítě, za použití odlišných nástrojů a aplikací

Tyto nedostatky se snaží odstraňovat tzv. adresářové služby, které se stávají nedílnou součástí moderních řešení podnikové infrastruktury. Adresářovou službou (Directory Service, DS) se rozumí aplikace, která umožňuje uchovávat informace o daných objektech informačního systému, dále pak tato data organizovat, přistupovat k nim a provádět s nimi různé operace.

Protokol LDAP

LDAP (Lightweight Directory Access Protocol) je odvozen od obecného standardu X.500. Specifikace protokolu LDAP je implementačně nezávislá a je vedena snahou o maximální jednoduchost. Díky tomu došlo k jeho značnému rozšíření, takže je v současné považován za průmyslový standard.

LDAP definuje dva typy autentizace (autentizační proces zpracovává informace, které udávají, jestli jsme ti, za něž se vydáváme) - **jednoduchou** autentizaci a **SASL** (Simple Authentication and Security Layer specification). První z uvedených jednoduše ověřuje správnost hesla k danému uživatelskému účtu, pod kterým se uživatel přihlašuje do systému. Toto spojení je tedy vhodné použít tehdy, když server obsahuje informace, které nevyžadují ochranu a my se nechceme zabývat otázkou přihlašování. Druhý typ (SASL) zajišťuje bezpečné připojení a je mnohem složitější. SASL spojení bylo definováno pro širokou oblast různých služeb. V praxi se ukazuje, že je velmi výhodné použít v případě, když potřebujeme použít větší zabezpečení, než které nám poskytuje jednoduchá autentizace.

Vrstva SSL (Secure Sockets Layer) řeší zabezpečení přenášených dat mezi klientem a serverem a je vložena mezi aplikační protokol a protokol TCP/IP. Přenášená data se pak tedy např. mezi WWW serverem a browserem přenášejí zakódovaně pomocí šifrování veřejným a tajným klíčem. Klíče navíc obvykle obsahují autentifikační informaci od certifikační autority (CA).

Správa identit - Identity Management

Využití adresářových služeb (LDAP) je však pouze jedním z kroků k centrálnímu uložení a efektivní správě uživatelských oprávnění k síťovým zdrojům a aplikacím. Je třeba hledat řešení pro správu identit, které poskytne soubor procesů a technologií pro řízení bezpečného přístupu k informacím a informačním zdrojům v organizaci. Umožní provádět správu identit centrálně, rychle, efektivně, a to při dodržení všech zásad definovaných bezpečnostní politikou organizace a platných zákonů pro ochranu osobních údajů. Všechny tyto požadavky splňují systémy, které se shodně označují pojmem Identity Management (IM). Správa identit je spojení adresářových služeb, zabezpečení sítě a autentizace, zaopatření a správy uživatelů, technologií pro jediné přihlášení se do systému (single sign-on, SSO) a webových služeb (web services).

Jednou větou lze tedy Identity Management systémy charakterizovat jako "efektivní řízení životního cyklu uživatelských identit s centralizovaným řízením pravidel a zdrojů, decentralizovanou administrací a samoobslužným přístupem uživatelů".

Téměř každý systém či aplikace má definovanou svou vlastní politiku pro přístup uživatelů, což s sebou přináší množství různých správců, nástrojů administrace a různá bezpečnostní pravidla. Cílem IM je sjednotit správu přístupů do jedné aplikace s jednotným rozhraním, která eliminuje rozdíly ve správě jednotlivých systémů. To umožní podstatné zjednodušení celého procesu přidávání, modifikace a mazání přístupových oprávnění, při naplnění bezpečnostních pravidel v organizaci.

Skupinu uživatelů se shodně nastaveným oprávněním definujeme jako »roli«. V IM systému jsou dány jednotlivé role podle typu přístupu nebo typu uživatele. Pro každou roli je pak možné stanovit pravidla (policy), která příslušné roli přiřazují odpovídající účty nebo oprávnění na spravovaných systémech. Změní-li se nastavení role, automaticky je tato změna aplikována na všechny osoby, které mají tuto roli přidělenou. Podobné je to se zrušením role, kdy jsou přístupová oprávnění automaticky odebrána. Řízení přístupu prostřednictvím rolí usnadňuje delegování pravomocí na jiné osoby, protože definované role jsou abstrahovány od konkrétních technických nastavení přístupových oprávnění a jsou srozumitelné i IT laikům.

Pro maximální využití možností, které IM poskytuje, je nutné provést analýzu, jejímž výsledkem je přesná definice rolí a odpovídajícího popisu.

Jedním ze základních prostředků IM je »workflow«. Slouží pro modelování procesů vedoucích k vytvoření požadovaného účtu či nastavení atributu při zachování všech formálních požadavků na takovýto proces v organizaci. Primárním cílem je umožnit schvalování požadavků definovaných uživateli IM při respektování organizační struktury a dalších pravidel. Tato pravidla mohou být stanovena i vně workflow.

»Delegace administrace« je důležitá oblast, která umožňuje přenesení odpovědnosti za určité operace v IM na osoby, které na to mají z titulu své funkce pravomoc. Není tedy již nutné, aby změny prováděli správci systémů nebo jiné specializované útvary. Odpovědnost je přenesena na přímého řídicího nebo pověřeného pracovníka, který spravuje danou oblast nebo útvar.

Speciální formou delegace jsou tzv. »samoobslužné služby« (SelfServices). Ty umožňují uživatelům, kteří mají přístup do IM aplikace, samostatně provádět změny atributů spojených se svou osobou, jako např. žádat o přidělení dalších zdrojů, případně modifikaci, či žádat o jejich zrušení. Veškeré tyto operace je možné individuálně povolovat či zakazovat prostřednictvím přístupových oprávnění k atributům či operacím IM. Pro většinu uživatelů však zůstává hlavní volbou SelfServices změna hesla.

IM systémy nabízejí možnost »centrální správy hesel« pro všechny definované účty. Na hesla je aplikována politika, která musí splňovat bezpečnostní požadavky všech integrovaných systémů. Uživatel si může prostřednictvím IM aplikace změnit hesla na kterémkoliv systému či aplikaci, ke kterým má přístup, a to pro všechny najednou, či jednotlivě. Stejnou volbu může realizovat správce systému nebo jiná pověřená osoba.

Závěr

Stále více podniků a organizací si uvědomuje důležitost efektivní a bezpečné správy uživatelských účtů a řada dodavatelů z oblasti IT na tuto poptávku reaguje různými specializovanými produkty, ale na trhu jsou i řešení, která se snaží o ucelený přístup k této problematice. Je vidět, že IM systémy značně zvyšují efektivitu správy identit v organizaci, úroveň bezpečnosti a v neposlední řadě i komfort uživatelů. I přes jejich nesporné výhody však přináší také potenciální rizika spojená s koncentrací citlivých informací do jednoho místa. Je tedy nutné v maximální možné míře IM systémy, a obzvláště jejich úložiště dat, chránit před zneužitím.

Ing. Jan Krejčí