

ORACLE DATABASE BEZPEČNOSTNÍ MECHANISMY

HLAVNÍ VLASTNOSTI

- Zajištění principu minimálních nutných práv
- Jemný mechanismus řízení přístupu pomocí systémových i objektových práv
- Řízení přístupu na úrovni záznamů
- Transparentní šifrování dat
- Šifrování záloh
- Šifrování komunikace
- Detailní audit operací
- Podpora autentifikačních služeb třetích stran a mechanismů vícefaktorové autentifikace
- Centrální správa uživatelů - spolupráce s LDAP
- Bezpečnostní certifikace

Oracle Database poskytuje širokou škálu bezpečnostních mechanismů, např. v oblasti řízení přístupu, šifrování či auditování, které ji předurčují pro použití i v prostředích s vysokými nároky na bezpečnost.

Důvěryhodnost implementace těchto mechanismů dokazuje i mnoho nezávislých bezpečnostních ohodnocení, která databázový server Oracle opakovaně úspěšně absolvoval.

Zajištění bezpečného provozu informačního systému je komplexní činností zasahující do všech komponent a dimenzí informačního systému. Protože většina cílů zajištění bezpečnosti souvisí s ochranou podnikových dat, hraje zde nezastupitelnou roli i efektivní zajištění bezpečnosti přímo na úrovni databázového serveru.

Proč ale vlastně řídit přístup a využívat další bezpečnostní mechanismy na úrovni databázového serveru, když to lze provádět i na úrovni vlastní aplikace?

- Pokud k datům přistupuje více aplikací jsou práva definována centrálně a není třeba je implementovat opakovaně v každé aplikaci. To snižuje riziko, že některá z implementací nebude dostatečně kvalitní
- Řízení přístupu i řada dalších bezpečnostních mechanismů je převážně deklarativní, nevyžadující programování. Lze tedy relativně jednoduše pomocí systémových pohledů kontrolovat správné nastavení – oproti tomu kontrolovat správnost řízení přístupu v kódu programu je značně problematické
- Dochází k minimalizaci rozsahu možného ohrožení dat v případě, že uživatel získá kontrolu nad aplikací samotnou – například tolik populární napadení pomocí SQL Injection může mít nulové, nebo jen minimální následky, pokud aplikace k databázi přistupuje přes uživatele s minimálními právy, která dovolují provést na úrovni databáze jen ty operace, které lze provést i přes aplikaci. Pokud ale aplikace přistupuje k databázi s právy vlastníka databázových tabulek nebo dokonce databázového administrátora, jsou vaše data nechána na pospas útočníkovi
- Na rozdíl od aplikace vyvíjené na míru pro jednoho zákazníka, je databázový server software, provozován stovkami tisíc zákazníků po celém světě. Bezpečnostní mechanismy databázového serveru tak jsou prověřené mnohaletým provozem v řadě značně rozdílných prostředí. Databázový server Oracle navíc úspěšně prošel řadou nezávislých bezpečnostních certifikací, včetně *Common Criteria for Information Technology Security Evaluation (ISO 15408)* na úrovni EAL-4.

Řízení přístupu

Databáze Oracle nabízí řadu různých jemně odstupňovaných systémových i objektových přístupových práv, kterými lze určovat, jaké operace uživatel provádět smí a jaké už ne. To odpovídá všeobecně uznávané zásadě přidělovat uživatelům pouze MINIMÁLNÍ NUTNÁ PRÁVA. Každé právo navíc znamená zvýšení rizika zneužití.

Snazší správě přístupu pomáhá klasický systém rolí. U nového zaměstnance není nutné procházet dlouhý seznam databázových objektů a přemýšlet jaký potřebuje přístup. Přidělí se mu takové role, které odpovídají jeho pracovnímu zařazení.

Co když je třeba uživateli přiřadit určitá práva pouze v případě, kdy k datům přistupuje z konkrétní aplikace? Jak zajistit, že uživatel může určité operace provádět jen pokud přistupuje z dané aplikace a nikoliv, pokud k přístupu použije třeba databázovou konzoli? Pro tyto účely je v databázi Oracle implementován mechanismus tzv. **Secure Application Role**. Tyto role jsou pevně svázané s určitou databázovou package (knihovnou uložených procedur) a mohou být aktivovány pouze z této package. V ní lze samozřejmě provést dodatečné kontroly a aktivovat roli jen, pokud uživatel splnil požadované podmínky.

S postupujícím trendem konsolidace se ukazuje potřeba řízení přístupu na mnohem detailnější úrovni, než jsou tradiční systémová a objektová práva. Jak zajistit, aby uživatelé z různých oddělení mohli pracovat pouze se svými daty, i když jsou data celého podniku ve stejné tabulce? Pro tyto účely bylo do databáze Oracle doplněno řízení přístupu na úrovni záznamů - **Virtual Private Database (VPD)**. VPD zajišťuje automatické a transparentní doplnění jakéhokoliv dotazu o bezpečnostní podmínku. Ta pak omezuje data, se kterými uživatel může pracovat. I když tedy dva uživatelé zadají stejný dotaz (například výpis celé tabulky), může každý získat jiná data (například jen data o jejich oddělení).

V řadě organizací se uplatňuje princip označování dokumentů i jiných dat bezpečnostními štítky určujícími úroveň jejich důvěrnosti (v nejjednodušším případě např. veřejné, důvěrné, tajné). Tento mechanismus je v databázi již přímo implementován pomocí **Oracle Label Security Option**. Každý záznam je označen štítkem určujícím jeho citlivost. Každý uživatel má na druhé straně definovány bezpečnostní úrovně se kterými může pracovat. Databáze Oracle pak zajistí, že uživatel může pracovat pouze s těmi daty, jejichž citlivost odpovídá jeho úrovni.

Identifikace a autentifikace uživatele

Základním mechanismem v oblasti autentifikace uživatelů je přihlášení pomocí jména a hesla. Nicméně stejně tak je možné využít i různé pokročilé metody implementované v rámci **Oracle Advanced Security Option (ASO)**, jako jsou třeba klientské SSL certifikáty, nebo využití různých autentifikačních služeb postavených na standardech Kerberos či RADIUS. Pomocí těchto služeb lze například zajistit ověřování pomocí různých elektronických karet nebo třeba biometrických údajů.

Problém s identifikací uživatelů však může nastat u webových aplikací a to díky rozšířenému postupu, kdy se aplikace do databáze přihlašuje stále pod stejným jménem a heslem. Databáze totiž neví, kdo s ním skutečně pracuje, což blokuje řadu jejích bezpečnostních funkcí. Pro tyto situace Oracle implementoval mechanismus **Proxy Authentication**, který aplikaci sice umožní přistupovat do databáze stále pod stejným jménem a heslem a ušetřit tak čas na vytvoření spojení, avšak zároveň dovoluje předat informace o skutečném uživateli, který s aplikací pracuje. Databázový systém pak tuto informaci využije při řízení přístupu i auditování.

Šifrování

Oproti přesvědčení laické veřejnosti zavedením šifrování není otázka zabezpečení systému vyřešena. Šifrování je jen jedním z celého spektra mechanismů, které je třeba vhodně zkombinovat.

Šifrování přenosu dat má za cíl zabránit odposlechnutí či dokonce pozměnění komunikace. Vedle SSL lze pro šifrování přenosu dat použít i některé další algoritmy obsažené v rámci **Advanced Security Option**. Šifrování komunikace je přitom transparentní pro samotnou aplikaci – zavedení šifrování je pouze otázkou konfigurace a neznamena nutnost zásahu do kódu aplikace.

Vedle toho poskytuje Oracle ve všech edicích databáze nástroje pro výběrové programové šifrování a dešifrování dat pomocí standardních algoritmů, jako je DES, 3DES, AES a MD5. Ty umožňují zašifrovat některá obzvláště citlivá data, jako jsou například rodná čísla, nebo čísla kreditních karet.

Advanced Security Option byla ve verzi 10g Release 2 rozšířena o šifrování dat v tabulkách, které je transparentní z pohledu aplikace – nevyžaduje tedy zásah do kódu aplikace. Šifrování dat se nastavuje deklarativně při definici tabulky. Tento mechanismus chrání před unikem dat při přístupu obcházejícím databázový server – např. kopírováním datových souborů, nebo zcizením záložních médií.

Audit operací

Nedílnou součástí bezpečnostních mechanismů je i možnost auditování operací prováděných jednotlivými uživateli. Základní auditovací mechanismy většinou vytvářejí velký objem záznamů a hledat v nich známky porušení či ohrožení bezpečnostních pravidel připomíná příslovečné hledání jehly v kupce sena. Proto Oracle implementoval tzv. **Fine Grained Auditing (FGA)**. FGA umožňuje detailně určit jakých dat se má operace týkat specifikací sloupce tabulky a podmínky. Pouze pokud se v rámci uživatelem prováděné operace začne pracovat se záznamem splňujícím podmínku a je vrácena informace z definovaného sloupce, je tato operace zapsána do auditovacího logu. Při takové události je možné spustit i uloženou proceduru, která zajistí patřičnou reakci – například zašle SMS správci databáze. Informace zapisované do auditovacího logu o byly rozčliveny o vlastní text prováděného dotazu. Spojení s mechanismy **Flashback** pak umožňuje získat i přesný výsledek dotazu v době, kdy byl daným uživatelem původně spuštěn, nebo obnovit data do podoby před útokem, aniž by bylo třeba využívat obnovu dat ze zálohy.

Správa uživatelů

Se vzrůstajícím počtem a složitostí systémů je čím dál obtížnější zajistit aktuální seznam uživatelů s jejich hesly a rolemi pro všechny komponenty. Často se stává, že při nástupu do zaměstnání musí být uživatel zaveden do řady systémů s různými rolemi. Nejen, že je tento proces náročný časově, ale je také náchylný k chybám. Skutečný problém pak znamená odchod zaměstnance – může se lehce stát, že se na některý systém zapomene. Celý problém se mnohonásobí ve chvíli, kdy řešíte nutnost zajistit přístup vašich partnerů či zákazníků do některých z vašich systémů. V tu chvíli je již správa uživatelů na úrovni jednotlivých komponent skutečně nemyslitelná.

Z těchto důvodů vznikl koncept centrální správa uživatelů. Správa uživatelů se provádí na jednom místě, ze kterého si jednotlivé aplikace přebírají data pomocí standardu LDAP. V prostředí Oracle funkci tohoto centrálního prvku plní **Oracle Internet Directory (OID)**.

Centrální správu uživatelů v OID lze samozřejmě využít i pro správu databázových uživatelů a rolí. Tato funkcionality je označena jako **Enterprise User Security**. Databáze může přebírat nejen seznam uživatelů, ale může z OID získat i seznam rolí

přiřazených uživatelů, se kterými lze pracovat stejně jako s běžnými databázovými rolemi. Oracle již ve verzi 8i umožnil vytvářet uživatele nezávisle na databázových schématech – více uživatelů založených v OID pak může sdílet jedno databázové schéma. To výrazně zjednodušuje správu. Běžní aplikační uživatelé totiž nepotřebují každý své databázové schéma. Využívají pouze prostředky dané aplikace, přistupují k objektům v rámci jednoho databázového schématu aplikace a nevytváří vlastní databázové objekty. To, že uživatelé nemají vlastní databázové schéma ale samozřejmě neznamená, že by je nebylo možné rozlišit – i nadále můžete řídit jejich přístup i využívat ostatní mechanismy databáze Oracle.

Závěr

Informační systémy jsou v současnosti ohrožovány řadami hrozeb a každým dnem přibývají nové metody útoku. Jedině správnou kombinací bezpečnostních opatření na všech úrovních systému lze minimalizovat riziko jejich napadení. Měrou pro nasazení těchto mechanismů a s tím souvisejícím hodnocení investic do zabezpečení by mělo být ohodnocení škod, které mohou potenciálně podniku vzniknout při ztrátě či úniku dat z daného systému. Celková míra zabezpečení systému však není dána jen použitým software, ale má i své další složky, z nichž velmi důležitou je rozhodně i organizační dimenze.