

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství



Teze bakalářské práce

Zabezpečení relačně databázových evidencí

Jindřich Novotný

©2015 ČZU v Praze

Souhrn

Cílem této bakalářské práce je objasnit teoretické principy relačně databázové technologie v kontextu s problematikou zabezpečení podnikových databází. Zmapovat aktuální stav a vymezit relevantnost dané problematiky. Na základě teoretických poznatků pak navrhnout konkrétní řešení. K řešení zvoleného problému je v této práci využita kombinace rolí a pohledů, jež slouží k tvorbě interního zabezpečení, dále pak profily, které jsou naopak používány při tvorbě externí bezpečnosti. Řešení vytvořené v rámci této práce napomáhá snížení rizika přístupu neautorizovaných osob k datům uloženým v relačních databázích, a to především díky přesnému vymezení kompetencí jednotlivých uživatelů a posílení bezpečnosti jejich účtů. Přínosem této práce je pak prokázání nutnosti vytváření bezpečných databázových systémů a porovnání jednotlivých technik, jež jsou k tomuto účelu nejčastěji využívány. Navržené řešení lze navíc použít jako návod, jak k problematice zabezpečení relačně databázových evidencí přistupovat.

Klíčová slova

relačně databázová technologie, oprávnění, role, pohledy, profily, SQL

Vlastní text

Cíl práce a metodika

Bakalářská práce je zaměřena na problematiku zabezpečení relačně databázových evidencí v podnikatelských subjektech. Hlavními cíli této práce pak je zmapovat momentální stav řešené problematiky a vymezit její relevantnost včetně požadavků na ni kladených. Objasnit teoretické principy relačně databázové technologie v kontextu s problematikou zabezpečení databázově evidovaných dat. Na základě teoretických poznatků pak navrhnout a ověřit řešení dané problematiky v souladu s identifikovanými požadavky a se zřetelem na reálné možnosti podnikatelských subjektů. Získané poznatky následně zobecnit pro další možná využití.

Metodika zpracování této bakalářské práce je založena na studiu a analýze dostupných informačních zdrojů a existujících řešení v dané oblasti. Hlavními informačními zdroji pak budou především odborné publikace pojednávající o problematice relačně databázové technologie a dokumentace Oracle. Stěžejní pro vypracování této závěrečné práce budou metody a techniky relačně databázové technologie využívané v kontextu s problematikou zabezpečení relačních databází podnikatelských subjektů. Navrhované řešení bude zohledňovat identifikované požadavky a očekávání spojená s řešenou záležitostí. Na podkladě syntézy teoretických poznatků a dosažených výsledků budou formulovány závěry této bakalářské práce a následně zobecněny pro další možná použití.

Teoretická východiska

Úvodní teoretická část bakalářské práce je rozdělena na tři kapitoly. První z teoretických kapitol blíže zkoumá relevantnost problematiky zabezpečení relačně databázových evidencí. Dále je v této kapitole popsáno, z jakých důvodů je třeba se danou problematiku zabývat, co ji definuje a jaké nároky jsou na ni kladené.

Následující kapitola objasňuje základní pojmy a principy relačně databázové technologie, jako jsou například relační datový model a jeho součásti či princip transakčního zpracování. Díky popisovaným prvkům relačně databázové technologie je možné vytvářet robustní databáze, které se následně mohou stát stabilní platformou, na níž lze poté vytvářet jednotlivé prvky zabezpečení.

Poslední z teoretických kapitol pak popisuje jednotlivá rizika hrozící databázím podnikatelských subjektů a jejich možné následky. Dále jsou zde definovány konkrétní nástroje a techniky sloužící v rámci relačně databázové technologie k vytváření bezpečnostních opatření, ty tvoří jádro celé bakalářské práce. Mezi popisovanými nástroji je možné nalézt oprávnění, role a pohledy, jež slouží k tvorbě interní bezpečnosti. Hlavním cílem kombinace těchto nástrojů je přesná definice kompetencí jednotlivých uživatelů, což umožní zabránit uživatelům v přístupu k datům, s nimiž nejsou oprávněni pracovat. Dalším z popisovaných nástrojů jsou pak profily, které jsou naopak využívány při tvorbě externí bezpečnosti. Hlavním účelem profilů je zvýšení bezpečnosti uživatelských účtů, díky čemuž lze snížit riziko napadení databáze způsobené získáním kontroly nad uživatelským účtem neautorizovanou osobou.

Praktická část

Druhá část bakalářské práce je věnována praktickým ukázkám, jež vystihují podstatu řešené problematiky a především ukazují konkrétní využití jednotlivých technik definovaných v teoretické části. Navrhované řešení pak spočívá v tvorbě funkčního prototypu databázového zabezpečení pro modelovou databázi fiktivní společnosti. V rámci navrhovaného prototypu je zkonstruováno několik pohledů a rolí, také je na něm demonstrováno nastavení profilu, včetně tvorby verifikační funkce. Poslední je pak ukázka životního cyklu uživatelského účtu, na němž je demonstrována úspora zdrojového kódu při použití rolí. K tvorbě a ověření funkčnosti navrhovaného řešení byl využit produkt Oracle Database 11g. Po praktických ukázkách jsou veškeré použité techniky srovnány a zhodnoceny za pomoci kvalitativních parametrů. Jako parametry pro srovnání použitých technik byly vybrány následující: náročnost na znalosti potřebné k realizaci jednotlivých technik, část zabezpečení, v níž jsou využívány a výsledný efekt, kterého je možné dosáhnout s využitím konkrétní techniky. Na závěr praktické části této bakalářské práce je pak uvedeno doporučení, kdy a za jakých podmínek je vhodné kterou z technik využít.

Zhodnocení a závěr práce

Na počátku vytyčené cíle bakalářské práce byly splněny, přičemž ze studia a analýzy vybraných informačních zdrojů a následného návrhu a zpracování vlastního řešení zvolené problematiky vyplynuly následující důležité poznatky.

Síla informací je v dnešní době ve společnosti obecně velmi ceněna. Zejména pak proto, že v tržně ekonomické společnosti jsou informace pro podnikatelské subjekty nezbytným zdrojem konkurenceschopnosti. A právě kvůli síle informací je třeba, aby data, jež jsou jejich nositelem, byla efektivně chráněna před možným zneužitím či poškozením. Pokud by snad došlo k narušení bezpečnosti, mohly by neautorizované osoby získat přístup k citlivým či strategicky významným datům, jež společnost eviduje ve svých databázích. Jestliže by nastala podobná situace a důležitá data by byla zcizena či poškozena, pro podnikatelský subjekt by to mohlo znamenat ztrátu důvěry svých klientů, konkurenceschopnosti nebo i právní kroky proti společnosti. Aby bylo možné zabránit podobným situacím, je nutné navrhovat co možná nejbezpečnější databázové systémy, zejména jedná-li se o databáze podniků evidujících data, jež by měla podléhat utajení.

Předtím, než je vůbec možné začít vytvářet jednotlivé prvky zabezpečení relačně databázové evidence, je nejprve nutné vytvořit robustní databázi, která dokáže odolat nejrůznějším kritickým scénářům a při tom zachovat relevanci dat. Takováto databáze se poté může stát stabilní platformou pro konkrétní řešení bezpečnosti. K zajištění stability navrhovaných evidencí se v rámci relačně databázové technologie využívají především prvky jako jsou transakční zpracování, integritní omezení a v neposlední řadě též vlastnosti relačních tabulek, jež tvoří základ relačně datového modelu.

Při návrhu bezpečnostních opatření pro konkrétní databázi je vždy nejprve nutné si odpovědět na následující otázky. Jak důležitá data se snažíme chránit? Kdo bude autorizován pro práci s databází, kterou se snažíme zabezpečit? Jaké budou kompetence jednotlivých uživatelů? Dále je třeba si uvědomit, jaká rizika mohou databázi reálně hrozit a odkud by mohlo dojít k narušení bezpečnosti. Zmíněné faktory ovlivňují jaké nástroje při tvorbě zabezpečení použijeme, ale také směr, jímž se bude následné vývoj konkrétního řešení bezpečnosti ubírat. Jestliže jsou zmíněné faktory správně zanalyzovány, je možné nastavit optimální míru zabezpečení. Díky správnému nastavení bezpečnostních prvků lze databázi efektivně chránit a zároveň zabránit snížení pracovní efektivity uživatelů. Zabezpečení se dělí na interní a externí, přičemž interní bezpečnost se věnuje otázkám řešícím problematiku vymezení kompetencí autorizovaných uživatelů databáze. Naopak externí bezpečnost řeší jakým způsobem zabránit neautorizovaným osobám v přístupu k databázi. Nejrozšířenějším nástrojem pro tvorbu interního zabezpečení jsou oprávnění, respektive role, jež jsou často kombinovány s pohledy za účelem zvýšení efektivity interní bezpečnosti. Tato kombinace umožňuje přesně vymezo-

vat kompetence jednotlivých uživatelů. Při tvorbě externího zabezpečení se pak velmi často využívají profily, které rozšiřují možnosti zabezpečení uživatelských účtů.

Relačně databázová technologie, jejíž základ vytvořil E. F. Codd již v roce 1970, je i dnes, po více než čtyřiceti letech, stále rozvíjena a přináší nové poznatky v problematice zpracování hromadných dat a především pak nové metody usnadňující tvorbu databázového zabezpečení. Původní technologie se postupně rozdělila na tři vývojové směry, kterými jsou relační, objektově-relační a čistě objektové databáze. Každý z těchto modelů má své výhody i nevýhody. Avšak i přes fakt, že objektově orientované technologie jsou dnes velice populární, zůstává relačně databázová technologie stále nejrozšířenější alternativou pro podnikové systémy, v nichž je třeba evidovat velké množství dat. Do budoucna se pravděpodobně budou stále více rozvíjet objektově orientované technologie, potrvá však ještě dlouho, než relační databáze zcela vymizí.

Použitá literatura

BRYLA, Bob a Kevin LONEY. Mistrovství v Oracle Database 11g. Computer Press 2010. ISBN: 978-80-251-2189-4

CONNOLLY, Tomas. Mistrovství Databáze - Profesionální průvodce tvorbou efektivních databází. Computer Press, 2009. ISBN: 978-80-251-2328-7

HERNANDEZ, Michael J. Návrh databází. GRADA, 2006. ISBN: 80-247-0900-7

LONEY, Kevin. Oracle database - Kompletní průvodce. Computer Press 2010. ISBN: 978-80-251-2489-5

OPPEL, Andy. Databases DeMYSTiFieD, 2nd Edition. McGraw-Hill Companies, 2010. ISBN: 978-0071747998

Oracle Database Help Center. Database documentation. [online]. 21.11.2014 [cit. 2015-01-12]. Dostupné z: <https://docs.oracle.com/en/database/>

POKORNÝ, Jaroslav a Michal VALENTA. Databázové systémy. Česká technika - vydavatelství ČVUT, 2013. ISBN: 978-80-01-05212-9

SHARMA N., PERNIU L., CHONG R. F., IYER A., NANDAN Ch., MITEA A. a NONVINKERE M. a DANUBIANU M. Database fundamentals. IBM, 2010. Dostupné z: http://public.dhe.ibm.com/software/dw/db2/express-c/wiki/Database_fundamentals.pdf

VOSTROVSKÝ, Václav. Vytváření databází v Oracle. Česká zemědělská univerzita v Praze, 2009. ISBN: 978-80-213-1191-6