TECHNIKA TRANSPORTU SZYNOWEGO

Eugenia BUSŁOWSKA

BEZPIECZEŃSTWO BAZ DANYCH

Streszczenie

W artykule zaprezentowano wybrane mechanizmy zwiększenia bezpieczeństwa baz danych. Omówiono aspekty bezpieczeństwa i sposoby ich zapewniania. Skupiono się na kilku wybranych zagadnieniach związanych z zabezpieczaniem systemu i samych danych. Mechanizmy bezpieczeństwa danych rozpatrzono pod kątem ograniczenia praw dostępu i ukrywania za pomocą szyfrowania.

WSTĘP

W Polsce problematykę ochrony baz danych reguluje zarówno ustawa o prawie autorskim i prawach pokrewnych, (gdy baza danych spełnia cechy utworu) [10] oraz Ustawa z dnia 27 lipca 2001 roku o ochronie baz danych [9]. Ustawa ta powstała w oparciu o Dyrektywę 96/9/WE Parlamentu Europejskiego i Rady z dnia 11 marca 1996 r., w sprawie ochrony prawnej baz danych [3].

W ustawie o ochronie baz danych została sformułowana definicja baz danych podlegających ochronie: „baza danych oznacza zbiór danych lub jakichkolwiek innych materiałów i elementów zgromadzonych według określonej systematyki lub metody, indywidualnie dostępnych w jakikolwiek sposób, w tym środkami elektronicznymi, wymagający istotnego, co do jakości lub ilości, nakładu inwestycyjnego w celu sporządzenia, weryfikacji lub prezentacji jego zawartości” [9].

Przyjmując, że „sporządzanie bazy danych wymaga zaangażowania znacznych zasobów ludzkich, środków technicznych i finansowych” [9], a samo tworzenie jest w celu późniejszego wykorzystywania i takie bazy „mogą być kopiowane lub można mieć do nich dostęp, ponosząc tylko ułamkową część kosztu potrzebnego do ich niezależnego sporządzenia” [9]. Wprowadzono mechanizmy ochrony, które przysługują niezależnie od tego, czy dana baza ma cechy utworu (w rozumieniu prawa autorskiego) czy też takich cech nie posiada [10]. Jeśli nie posiada cech utworu, przysługuje ochrona samoistna *(sui genesis)*, zapewniająca ochronę inwestycji dokonanej w celu uzyskania, zweryfikowania lub prezentowania zawartości bazy danych [3].

Warunkiem objęcia prawnoautorską ochroną bazy danych jest tylko oryginalność utworu w sensie intelektualnej twórczości autora, przy czym nie stosuje się kryteriów estetycznych lub jakościowych. Ochrona wynikająca z przepisów prawa autorskiego nie wymaga, by baza danych miała jakąkolwiek wartość ekonomiczną. Ochrona bazy danych jest niezależna od ochrony poszczególnych części składowych. Bazę danych mogą stanowić utwory, które podlegają ochronie prawa autorskiego (np. utwory literackie, artystyczne, muzyczne) lub zbiory innych materiałów, takich jak: teksty, dźwięki, obrazy, liczby, fakty, dane lub inne materiały. Jeśli jednak sposobowi doboru elementów bazy danych, ich zestawieniu (nawet,

jeśli same w sobie nie mają charakteru twórczego i nie można uznać ich za utwory) można przypisać cechy działalności twórczej o indywidualnym charakterze - wówczas taka baza danych będzie utworem. Ustawa o prawie autorskim i prawach pokrewnych mówi, że: „zbiory, antologie, wybory, bazy danych, spełniające cechy utworu są przedmiotem prawa autorskiego, nawet jeśli zawierają niechronione materiały, o ile przyjęty w nich dobór, układ, zestawienie, ma charakter twórczy" [10]. Jeśli baza danych ma cechy utworu w rozumieniu prawa autorskiego i jest dostępna przy pomocy środków elektronicznych, to ochronie nie podlega program komputerowy używany do sporządzenia lub obsługi.

Prawo autorskie chroni jedynie specyficzny, twórczy wybór, układ i zestawienie zgromadzonych informacji, ale nie zabrania pobierania zebranych w bazach informacji. Specjaliści w zakresie prawa własności intelektualnej uznali, że interes producentów baz danych zasługuje na dodatkową ochronę. Przyjęte prawo *sui genesis*, ma zabezpieczyć producentów przed nieuczciwym przywłaszczeniem wyników ich finansowych i zawodowych inwestycji, poniesionych w celu utworzenia systemu bazodanowego [3].

Zgodnie z ustawą producentem bazy danych może być osoba fizyczna, prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która sama sporządziła bazę albo zawarła stosowne umowy, efektem, których było powstania bazy. Jeżeli baza danych jest efektem pracy wielu osób, współudziały są równe. Jest również możliwość ustalenia, kto i jaki miał wkład w tworzenie bazy, wówczas udziały są odpowiednie do poniesionych nakładów. Ustawa umożliwia przekazanie praw do bazy danych następcy prawnemu producenta bazy danych. Nie jest narzucona minimalna wielkość zbioru, który będzie określany mianem baza danych, czyli uporządkowany wedle określonej systematyki lub metody. Prawo do ochrony bazy danych przysługuje producentowi przez okres 15 lat następujących po roku, w którym została sporządzona. W przypadku dokonania istotnych zmian w treści, mających znamiona nowego nakładu, to okres ochrony liczy się od nowa. Producent bazy udostępnionej publicznie nie może zabronić użytkownikom pobierania lub wtórnego wykorzystania w jakimkolwiek celu nieistotnej, co, do jakości lub ilości, części jej zawartości. W przypadku naruszenia bazy danych przez użytkownika lub konkurenta, poprzez czynności dotyczące całości lub istotnej części zawartości bazy danych, zgodnie z ustawą może od niego zażądać [9]:

- zaniechania naruszenia,
- usunięcia skutków naruszenia,
- naprawienia wyrządzonej szkody (na zasadach ogólnych, bądź też poprzez zapłatę sumy pieniężnej należnej tytułem udzielenia przez uprawnionego zgody na korzystanie z baz danych),
- wydania uzyskanych korzyści, wynikających z korzystanie z bazy danych w celach majątkowych, bez uzyskania odpowiednich uprawnień, bądź też wbrew ich warunkom, grozi kara grzywny.

1. SYSTEMY BAZODANOWE

Niezawodne, szybkie i bezpieczne przetwarzanie ogromnych ilości danych jest dzisiaj strategicznym czynnikiem funkcjonowania większości instytucji. Dzięki pracom prowadzonym przez kilka ostatnich dziesięcioleci, powstało wyspecjalizowane oprogramowanie zwane systemem zarządzania bazą danych (*ang*. *Database Management System*, *DBMS*). Jest to zestaw rozbudowanych narzędzi do wydajnego tworzenia dużych zbiorów informacji wg określonego zbioru zasad (opisujących strukturę danych oraz dozwolone operacje) i zarządzania nimi.

Baza danych, jako kontener do przechowywania jest jednym z głównych składników wszystkich obecnie stosowanych systemów informatycznych. Najczęściej wykorzystywanym sposobem gromadzenia danych w bazie jest model relacyjny, w którym dane są

przechowywane w tabelach opisujących pojedyncze obiekty (osoby, przedmioty, czynności, zdarzenia, zjawiska) bądź związki pomiędzy obiektami. Każda tabela ma arbitralnie określoną liczbę kolumn i dowolną liczbę wierszy zwanych rekordami. Na przecięciu każdej kolumny z każdym wierszem występuje określona wartość prosta. Każda relacja ma zdefiniowany klucz główny, który stanowi pojedyncza kolumna lub zbiór kolumn, których wartości jednoznacznie identyfikują dany rekord. Wyszukiwanie danych odbywa się poprzez odwołanie do danego klucza i wybór wierszy za jego pomocą. Bazę danych stanowią, więc uporządkowane dane, posiadające własną strukturę i wartość [4].
Do wiązania ze sobą danych przechowywanych w różnych tabelach używa się kluczy obcych. Klucz obcy to kolumna lub grupa kolumn tabeli, o wartościach z tej samej dziedziny, co klucz główny tabeli z nią powiązanej. Rozwiązanie to umożliwia łatwy dostęp do danych, ich modyfikację, dodawanie nowych oraz usuwanie starych danych.
Oprogramowanie zarządzające dostępem do bazy danych oferuje:

- organizowanie struktury danych,
- wprowadzanie, usuwanie i aktualizowanie danych,
- wyszukiwanie danych według zadanych kryteriów,
- zachowanie integralności,
- niezależność danych,
- zabezpieczenie danych i ich spójność,
- administrowanie danymi,
- natychmiastowy i współbieżny dostęp do danych,
- zróżnicowane interfejsy,
- organizowanie pracy wielodostępowej,
- łączenie i wymianę danych z innymi systemami baz danych,
- zarządzanie transakcjami (zbiorem poleceń, które muszą się albo wszystkie wykonać poprawnie, albo w całości zostać wycofanymi, aby można było zapewnić spójność danych) [5, 6].

Najczęściej systemy bazodanowe mają architekturę scentralizowaną bądź też rozproszoną. Obie architektury posiadają swoje wady i zalety. Scentralizowana architektura przy projektowaniu nowoczesnych systemów informatycznych powoli ustępuje miejsca architekturze rozproszonej, jednak nadal ma szerokie zastosowanie. Zdecydowaną zaletą architektury scentralizowanej jest możliwość dysponowania centralną i zintegrowaną bazą danych, która może być udostępniona dla wszystkich użytkowników oraz wykonywanie wszystkich operacji w czasie rzeczywistym. Pierwsze tego typu systemy monolityczne (*ang. mainframe*) przetwarzały dane wyłącznie na jednym komputerze. Nie dawały one możliwości współdzielenia swoich zasobów z innymi systemami. Różne systemy potrzebowały dostępu do tych samych danych, w związku z tym wszystkie instytucje musiały przechowywać w wielu systemach nadmiarowe kopie danych. Rozwiązanie to było niewydajne i mocno kosztowne, więc szybko ustąpiło miejsca systemom wielowarstwowym.

Systemy wielowarstwowe to systemy dwuwarstwowe, typu klient – serwer, trójwarstwowe (klient, serwer aplikacji, serwer bazy danych) oraz internetowe systemy wielowarstwowe (przeglądarka, serwer WWW, serwer aplikacji, serwer bazy danych) [4].

Architekturę dwuwarstwową stanowi system bazy danych i oprogramowanie klienckie. We współczesnych dużych systemach baz danych, klient jest programem żądającym obsługi pewnego zlecenia, serwer jest programem odbierającym od klienta żądanie i wykonującym je. Najczęściej stosowanymi systemami zarządzania bazami danych opartymi o architekturę klient-serwer są: Oracle, Microsoft SQL Server, PostgreSQL, MySQL, DB2 firmy IBM i Sybase.

W architekturze trójwarstwowej występuje dodatkowa warstwa w postaci serwera aplikacji. Głównym zadaniem trójwarstwowej architektury jest przeniesienie pewnych funkcji odnoszących się do zarządzania i przetwarzania informacji na stronę serwera tak, aby aplikacje klienckie realizowały zadania bez bezpośredniego dostępu do danych.

W architekturze wielowarstwowej między serwerem bazy danych a programem klienckim jest program pośredniczący w postaci serwera WWW. Obecnie realizacje internetowych baz danych odbywają się na platformie UNIX/Linux i są to rozwiązania darmowe oraz na platformie Windows, w rozwiązaniach komercyjnych.

Rozproszoną architekturę stanowią współpracujące ze sobą lokalne bazy danych, znajdujące się na różnych serwerach i w różnych miejscach. Wszystkie te bazy są identyfikowane unikalna nazwą globalną i razem stanowią całość w sensie modelu danych oraz koordynacji wykonywanych transakcji [11].

2. BEZPIECZEŃSTWO BAZ DANYCH

Przechowywane dane w bazach danych mogą być narażone na wiele rodzajów zagrożeń. Do najważniejszych zaliczamy:

- nielegalny odczyt danych przez nieuprawnionych użytkowników,
- niepoprawne operacje zmiany danych, które mogą być skutkiem:
  - umyślnego działania nieuprawnionych użytkowników,
  - nieumyślnych pomyłek użytkowników,
  - braku właściwej kontroli przy wilodostępie,
  - błędów oprogramowania lub awarii systemów komputerowych,
- zniszczenie danych w wyniku awarii sprzętu komputerowego.

Rozpatrując bezpieczeństwo baz danych rozumie się zabezpieczanie przed nieuprawnionym, nieprawidłowym, przypadkowym lub umyślnym ujawnieniem, modyfikacją lub zniszczeniem. Zapewnienie bezpieczeństwa danym oznacza spełnienie kilku wymagań związanych z właściwościami systemu bezpiecznego. Bezpieczny system informatyczny to taki system, który zapewnia [1, 8]:

- poufność,
- integralność,
- dostępność,
- spójność,
- rozliczalność,
- autentyczność,
- niezaprzeczalność,
- niezawodność.

Poufność danych jest to brak możliwości ujawnienia osobom nieupoważnionym. Do naruszenia poufności może dojść na drodze bezpośredniego dostępu do informacji niejawnej (na przykład odczytania pliku, podsłuchania transmisji). Poufność może być naruszona także w wyniku tzw. dostępu pośredniego. W tym przypadku ujawnienie informacji chronionej jest skutkiem wnioskowania i analizy innych informacji, które nie podlegają ochronie. Wykorzystać można na przykład arytmetyczne i logiczne zależności między danymi jawnymi i niejawnymi. Mamy tu do czynienia z tzw. agregacją informacji.

Zapewnienie poufności informacji jest związane z ochroną prywatności i interesów własnych osób lub instytucji oraz obowiązującymi aktami prawnymi. W celu zapewnienia poufności stosuje się procedury uwierzytelniania poprzez tworzenie kont użytkowników. Każdemu kontu nadaje się uprawnienia związane tylko z wykonywanymi obowiązkami służbowymi. Ograniczając dostęp fizyczny do bazy danych lub szyfrując dane również zapewnia się ich poufność.

Integralność to pewność, że dane nie są podatne na żadne nieautoryzowane modyfikacje, podmienienie czy zniekształcenie. Dane otrzymywane przez adresata są zgodne z danymi autora. W celu zapewnienia integralności są stosowane sumy kontrolne danych (np. fizycznych plików) lub funkcje skrótów. Ograniczenie dostępu osób niepowołanych poprzez zastosowanie środków fizycznych w postaci serwerowni z ruterami i serwerami, zamykanych na klucz, wpływa również na integralność. Wprowadzanie zmian ustala się tylko i wyłącznie z określonych aplikacji. W przypadku pojawiania się błędów oprogramowanie wykrywa je i koryguje. Kiedy dane atakują wirusy, oprogramowanie antywirusowe działa jak system immunologiczny środowiska danych, chroniąc je przed niepożądaną infekcją.

Aspekt dostępności oznacza możliwość korzystania z zasobów systemu przez osoby upoważnione, w zakresie posiadanych przez nie praw dostępu. Stosując kryptografię zwiększa się szybkość lokalizacji danych. Można wówczas zrezygnować ze ścian ogniowych. Dostępność musi być zagwarantowana podczas przechowywania, przesyłania i przetwarzania danych. Niestety każdy z tych etapów wymaga użycia innych środków ochrony do zapobiegania naruszeniom oraz wykrywania naruszeń.

Spójność dotyczy danych gromadzonych w bazie danych. Stan bazy danych jest nazywany spójnym, jeśli wszystkie dane, które zawiera baza danych, w tym momencie, mogą występować w świecie rzeczywistym. Wszelkie zmiany w bazie danych stanowią proces dyskretny. Wprowadzane, aktualizowane i usuwane informacje muszą spełniać warunki narzucone na dane podczas definicji bazy danych tak, by baza była zgodna z modelowaną rzeczywistością. W każdym momencie czasu baza danych znajduje się w pewnym stanie. Stan nazywamy spójnym, jeżeli wszystkie wartości, które zawiera baza danych w tym stanie mogą zaistnieć w świecie rzeczywistym. Warunki spójności mogą być dynamicznymi lub statycznymi. Warunki dynamiczne różnią się od statycznych tym, że pamiętają poprzedni stan. Zachodzenie warunków spójności zapewnia poprawność bazy danych. Naruszenie spójności danych następuje w wyniku semantycznie niepoprawnych operacji, niewłaściwej synchronizacji działania transakcji współbieżnych lub w wyniku awarii systemu [7, 8].

Przez bezpieczeństwo informacji należy rozumieć również zachowanie rozliczalności, autentyczności, niezaprzeczalności i niezawodności. Rozliczalność polega na zapewnieniu, że określone działania użytkownika mogą być przypisane w sposób jednoznaczny tylko jemu. Inaczej mówiąc brana jest odpowiedzialność za wykorzystanie systemu informacyjnego.
Autentyczność dotyczy użytkowników, procesów i informacji. Autentyczność polega na sprawdzaniu tożsamości podmiotów i prawdziwości zasobów.
Niezaprzeczalność oznacza brak możliwości zaprzeczenia swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie.
Niezawodność gwarantuje spójność danych i systemu oraz oczekiwane jego zachowanie i spodziewane wyniki [7, 8].

3. MECHANIZMY ZABEZPIECZANIA BAZ DANYCH

Bazę danych zabezpieczamy jedynie przy uzasadnionej potrzebie ograniczania dostępu do wybranych lub wszystkich zgromadzonych w niej zasobów. System zabezpieczeń powinien gwarantować odpowiednią do zastosowania kontrolę dostępu do danych, przy zapewnieniu aspektów bezpieczeństwa, jak i dostateczny poziom wydajności użytkowej systemu.

Pierwszym elementem zabezpieczenia jest właściwe umiejscowienie serwerów bazodanowych w infrastrukturze instytucji. Poziom kontroli serwerów przez administratorów, to sprawa dość istotna, ale sama lokalizacja bazy nie gwarantuje od razu bezpieczeństwa. Największym błędem systemów bazodanowych jest ich domyślna instalacja. Po instalacji bardzo często administratorzy nie przeprowadzają żadnych zmian w mechanizmach zabezpieczeń. Niektóre instrukcje dotyczące bezpieczeństwa zostają niewłaściwie zinterpretowane a następnie wdrożone, co skutkuje włamaniami. Po instalacji pozostawienie

domyślnych kont i haseł sprawia łatwość dostania się do systemu i utworzenie do niego tylnych drzwi.

3.1. Ochrona systemu

Rolą każdego administratora jest ochrona systemu poprzez tworzenie kont użytkowników i nadawanie haseł. Hasła nie mogą być generowane losowo, ponieważ użytkownicy mają problem z ich zapamiętaniem i zapisują w różnych miejscach, często publicznie dostępnych. Hasła nie mogą być zbyt często zmieniane z wymogiem niepowtarzalności, co trzy, cztery hasła. Jednak bez narzuconej złożoności, hasła stają się trywialnymi. Dobrym rozwiązaniem jest podłączenie baz danych do systemu wprowadzania nowych haseł. System kontroluje podstawowe ułomności pseudolosowości ludzkiej, wykluczając imiona najbliższej rodziny, domowych pupili, daty urodzeń, adresy i inne hasła bezpośrednio związane z użytkownikiem.

Dla każdego konta użytkownika przydzielane jest miejsce na dysku dla jego obiektów i określane są ograniczenia do korzystania z różnych zasobów systemu, dostępnych dla danego użytkownika. Realizuje się to poprzez nadawanie odpowiedniego profilu. Jeśli przy tworzeniu użytkownika nie zostanie przypisany mu żaden profil domyślnie zostanie przydzielony profil Default. Profil domyślny nie ma ograniczeń na zasoby. Jednak powinien być zmieniony, tak, aby żaden użytkownik nie miał nieograniczonego dostępu do zasobów. Profile mogą służyć do nadawania limitów ilości zasobów systemu i bazy danych dostępnych użytkownikowi. Nakładają ograniczenia na zasoby jądra systemu tak, aby jeden użytkownik nie zajął całych zasobów poprzez ograniczenie użycia zasobów na poziomie sesji lub odwołanie. Odłączenie po odpowiednio długim czasie oczekiwania w sesji oraz wylogowanie użytkowników, jeśli nie pracują. Wszystkie ograniczenia są reakcyjne – żadna akcja nie występuje przed przekroczeniem limitu zasobu. Profile nie mogą wiec wspomagać zapobieganie wykorzystania przez niekontrolowane zapytanie dużych ilości zasobów systemowych przed wyczerpaniem określonego limitu. Profile również pozwalają na zarządzanie hasłami i określanie poprawnej polityki haseł. W profilu można określić liczbę kolejnych nieudanych prób zalogowania, po przekroczeniu, której nastąpi zablokowanie hasła, co uchroni przed próbami logowania aż do skutku. Można ustawić czas ważności hasła lub okres tymczasowej ważności hasła, czyli czas na dokonanie jego zmiany oraz ile razy trzeba zmienić hasło przed ponownym wykorzystaniem już użytego hasła. Podając nazwę funkcji wykorzystanej do oceny złożoności hasła można narzucić długość hasła i wymóg stosowania znaków specjalnych.

Konto i profil pozwalają na ochronę systemu poprzez sprawdzenie nazwy i hasła użytkownika, określenie, czy użytkownik ma prawo połączenia się z bazą, określenie ograniczeń zasobów dla użytkownika oraz możliwość monitorowania operacji systemowych użytkownika.

3.2. Ochrona danych

Oprócz ochrony systemu muszą być chronione same dane. Najistotniejsza jest kontrola dostępu do bazy danych i jej obiektów poprzez nadawanie użytkownikom odpowiednich uprawnień do wykonywania określonych operacji, ograniczanie dostępu i możliwości zmiany danych, ograniczanie możliwości wykonywania funkcji systemowych i zmian struktur bazy danych, nadawanie uprawnień: pojedynczym użytkownikom i rolom oraz wszystkim użytkownikom. Uprawnienia użytkownikom nadaje się w zależności od zajmowanego stanowiska i wykonywanych czynności. Zawsze jednak nadawanie uprawnień odbywa się od nadania minimalnych uprawnień i stopniowe, wg potrzeb, ich rozszerzanie. Przywileje bazodanowe to prawa do wykonywania określonych czynności na strukturze lub danych bazy

przez uprawnionych użytkowników. Przywileje stanowią dwie grupy: systemowe i obiektowe. Przywileje systemowe (*ang. system privileges*) – odnoszą się do całej bazy danych i określają prawa użytkownika do wykonywania dopuszczalnych operacji na jej obiektach. Przywileje obiektowe (*ang. object privileges*) - wyznaczają dostęp do danych bazy danych, na których uprawnione operacje mogą być wykonywane.

Użytkownik otrzymując uprawnienia systemowe otrzymuje prawo wykonania określonej akcji w bazie danych lub wykonania określonej operacji na wskazanym typie obiektu we wskazanym schemacie lub całej bazie danych. Przywileje systemowe nie specyfikują konkretnych obiektów. Wśród uprawnień systemowych są uprawnienia do: utworzenia sesji w bazie danych, tworzenia relacji w dowolnym lub tylko własnym schemacie, wydawania zapytań, usuwania obiektów i wiele innych.

Uprawnienia obiektowe wiążą się z przyznaniem użytkownikowi prawa wykonywania określonych operacji języka SQL tj.: ALTER, DELETE, EXECUTE, INDEX, INSERT, SELECT, UPDATE, na określonym obiekcie.

Uprawnienia użytkownikowi nadaje się bezpośrednio lub poprzez role. Role to zbiór uprawnień systemowych, obiektowych lub innych ról. Rolę można nadać tak jak uprawnienie, a w wyniku przyznania następuje równocześnie nadanie odbiorcy wszystkich uprawnień zawartych w roli. Tworzy się je dla grup użytkowników wykonujących na bazie danych podobne operacje związane ze stanowiskiem pracy. Upraszczają zarządzanie uprawnieniami dla dużych zbiorów użytkowników, ponieważ zmieniając uprawnienia należące do roli, zmienia się uprawnienia wszystkich użytkowników do niej przypisanych.

Dostęp do danych można ograniczyć stosując perspektywy (*ang. View*), inaczej wirtualne tabele. Wirtualne tabele udostępniają użytkownikowi tylko podzbiór rekordów lub atrybutów pojedynczej lub wielu tablic rzeczywistych. Udostępniane dane mogą być sformatowane i przedstawione w czytelniejszy sposób niż zostały wprowadzone do bazy. Mogą zawierać często używane przekroje danych lub ułatwiać pobieranie rezultatów złożonych zapytań. Do perspektyw mogą być przyznawane użytkownikom prawa dostępu nie przyznając tych praw do tablic rzeczywistych. Dzięki czemu można wprowadzić ograniczenia na dostęp do wybranych kolumn lub też wybranych wierszy tablic.

Mechanizmy bezpieczeństwa danych zwykle wpisują się w lokalne polityki bezpieczeństwa. W odniesieniu do danych wymagane jest rejestrowanie przetwarzania informacji, kontrolowanie wprowadzania, usuwania i wszelkich jej zmian. Obecnie w aplikacjach kontrolę dostępu użytkowników do danych można ustawić prawami dostępu na poziomie pojedynczego wiersza wybranej tabeli określonego użytkownika. Definiuje się, który użytkownik bazy ma dostęp, do jakiego podzbioru danych. Każde zapytanie będzie wykonywane po sprawdzeniu, czy występujące w zapytaniu tabele nie są chronione regułami polityk bezpieczeństwa. W zależności od przynależności użytkowników do grup, klauzula WHERE posiada odpowiednio dodatkowe warunki. Operacje te wykonywane są wewnątrz motoru bazy danych i są praktycznie niemożliwe do obejścia. Budowa takiego kompleksowego mechanizmu zabezpieczania danych to nowe zadanie stawiane projektantom systemów informatycznych z baza danych.

Dodatkowym mechanizmem zabezpieczania danych może być utajnianie kodu niektórych obiektów baz danych takich jak: procedury pamiętane, funkcje i pakiety. Utajnianie polega na obfuskacji (zaciemnianiu kodu) mającej na celu, takie przekształcenie kodu, aby zachowując jego działanie semantyczne utrudnić maksymalnie jego zrozumienie lub odczytanie. Zmieniony kod może być kompilowany i wykonywany tak jak każdy inny kod, lecz jest chroniony przed zamierzoną lub niezamierzoną modyfikacją. Gdy jest zaciemniony obiekt, to zmienia się tylko jego ciało. Specyfikacja obiektu pozostaje niezmieniona. Pozwala to na sprawdzenie jak można użyć obiekt, ale nie można podejrzeć jego implementacji. Kod nie może być edytowany. Jeśli zajdzie konieczność wprowadzenia zmian, trzeba wprowadzić zmiany w kodzie oryginalnym i ponownie zaobfuskować. Zanim użytkownicy otrzymają

obiekt trzeba pamiętać, że żadna metoda zaciemniania nie jest w stanie stuprocentowo uniemożliwić zrozumienie kodu, a jedynie znacznie utrudnia ten proces.

Ostatnią linią obrony w bazach danych jest zastosowanie mechanizmów kryptograficznych. Konieczność szyfrowania danych wynika często z przepisów prawa (ochrona danych osobowych) lub wymagań branżowych (PCI-DSS). Może ono dotyczyć szyfrowania zawartości plików, jako całości, bądź też poszczególnych rekordów lub kolumn. Przy szyfrowaniu wybranych kolumn dane są kodowane przed zapisaniem ich na nośnik danych. Jest to szyfrowanie transparentne (*ang. Transparent Data Encryption***)**. TDE zapewnia ochronę przed odczytaniem danych przy nieuprawnionym dostępie fizycznym np. po utracie kontroli nad dużymi zbiorami danych (kradzieży serwera, dysków lub kopii zapasowych).
W Microsoft SQL Server szyfrowanie TDE jest dostępne od wersji 2008. Dane są szyfrowane kluczem symetrycznym, który jest przechowywany w zaszyfrowanej bazie, ale również w postaci zaszyfrowanej. Oracle wprowadził TDE w wersji 10g R2, klucze kryptograficzne są przechowywane w "portfelu", który tworzy się określając jego lokalizację. Dostęp do "portfela" jest również chroniony za pomocą hasła.
Szyfrowanie w Microsoft SQL Server udostępnia nowoczesne algorytmy kryptograficzne AES do 256 bitów i 3DES. W Oracle jest realizowane algorytmem DES z kluczem o długości 56 znaków, 3DES z kluczem o długości 168 znaków i z kluczem o długości 112 znaków, AES z kluczem o długości 128, 192 i 256 znaków. W Oracle 11g dodano nową metodę szyfrowania danych (*ang. Transparent Tablespace Encryption*, TTE), będąca rozszerzeniem TDE. Technologia TTE jest bardziej wydajną metodą szyfrowania danych na poziomie całych przestrzeni tabel. Również i w tym wypadku są stosowane klucze szyfrujące.

Niezależnie od stosowanego mechanizmu szyfrowania niezwykle istotne jest stworzenie i przechowywanie w bezpiecznym miejscu kluczy pozwalających na odtworzenie zaszyfrowanej bazy. Dobrym rozwiązaniem jest przechowywanie stosowanych kluczy kryptograficznych w zewnętrznym module kryptograficznym.

PODSUMOWANIE

Wybierając mechanizmy bezpieczeństwa baz danych należy postawić pytanie jak cenne są dane i jakie koszty możemy ponieść na ich ochronę. Trzeba przewidzieć, które dane i przed kim powinny być chronione. Jakich ewentualnie zagrożeń możemy się spodziewać? Jacy są potencjalni napastnicy i ich motywacje oraz jakich metod mogą użyć by osiągnąć swój cel? Polityka zabezpieczania danych powinna być inna w przypadku banku, sklepu internetowego czy własnej strony z bazą danych. Bez dokładnego zrozumienia zagrożeń i znalezienia odpowiedzi na pytania, jak i dlaczego powinniśmy chronić dane, może się okazać, że stosowane metody nie są adekwatne do zagrożeń, które albo nam nie grożą, albo nie mogą być usunięte przy ich pomocy. Zabezpieczenie bazy danych przed szkodliwym działaniem użytkowników wewnętrznych wymaga podjęcia zupełnie innych kroków aniżeli próba sprostania atakom zewnętrznym. Zanim sięgniemy po szyfrowanie danych, jako najlepszą metodę ochrony, sprawdźmy czy na pewno ją potrzebujemy.

Artykuł powstał w ramach pracy badawczej S/WI/5/08 na Wydziale Informatyki Politechniki Białostockiej.

DATABASE SECURITY

Abstract

The article presents selected methods of increasing databases security. Aspects of the security and ways of providing it were described. The article concerns the chosen issues connected to the security

the system and the data. Mechanisms of data security examined for limiting the rights of access and concealment by encryption.

BIBLIOGRAFIA

1. Chałon M.: *Ochrona i bezpieczeństwo danych oraz tendencje rozwojowe baz danych*, Oficyna Wydawnicza Politechniki Wrocławskiej, 2007.
2. Date C. J.: *Relacyjne bazy danych dla praktyków*, Gliwice, Helion, 2005.
3. Dyrektywa 96/9/WE Parlamentu Europejskiego i Rady z dnia 11 marca 1996 r. w sprawie ochrony prawnej baz danych, L 77/20, Dziennik Urzędowy Wspólnot Europejskich, 27.3.1996.
4. Elmasri R., Navathe S. B.: *Wprowadzenie do systemów baz danych*, Helion, Gliwice, 2005.
5. Garcia-Molina H., Ullman J. D., Widom J.: *Systemy baz danych. Kompletny podręcznik*, Helion, wyd. II, Gliwice, 2011.
6. Mrówka-Matejewska E., Stencel K., Banachowski L.: *Systemy baz danych. Wykłady i ćwiczenia*, PJWSTK, 2004.
7. Pieprzyk J., Hardjono T., Seberry J.: *Teoria bezpieczeństwa systemów komputerowych*, Gliwice, Helion, 2005.
8. Stokłosa J., Bilski T., Pankowski T.: *Bezpieczeństwo danych w systemach informatycznych*, Księgarnia PWN, 2001.
9. Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych. (Dz. U. z dnia 9 listopada 2001r.), Dz.U.2001.128.1402.
10. Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, Dz.U.2000.80.904
11. Wrembel R., Bębel B.: *Oracle. Projektowanie rozproszonych baz danych*, Helion, Gliwice, 2003.

Autor:
dr inż. Eugenia BUSŁOWSKA –Politechnika Białostocka, Wydział Informatyki,
15-351 Białystok, ul. Wiejska 45A, tel. 85-746-90-50, Fax: 085-746-90-57,
e-mail: e.buslowska@pb.edu.pl