Bezpieczeństwo danych w bazach danych

Bardzo często w bazach danych przechowywane są wrażliwe i cenne dane. Gdyby wpadły one w niepowołane ręce lub bezpowrotnie przepadły, konsekwencje mogłyby być fatalne. Z tego też powodu istnieje wiele metod i mechanizmów mających na celu ochronę danych przed ich kradzieżą czy utratą. Zostały one opisane w niniejszym referacie.

Fizyczne bezpieczeństwo baz danych

Serwer, na którym znajduje się baza danych powinien znajdować się w bezpiecznym, zamkniętym miejscu, do którego nie mają dostępu osoby niezaufane i nieupoważnione. W przeciwnym wypadku, pomimo stosowania nawet najbardziej wyrafinowanych mechanizmów ochrony danych, mogą one zostać ukradzione lub zniszczone poprzez na przykład fizyczne wymontowanie dysku z maszyny.

Ponadto, te same dane powinny być przechowywane przynajmniej w dwóch różnych lokalizacjach. Kopie zapasowe mają na celu ochronę przed bezpowrotną utratą danych spowodowaną np. awarią sprzętu, klęskami żywiołowymi, pożarami, atakami terrorystycznymi itd.

Ponadto, bazy danych nie powinny być umieszczone na maszynach, do których istnieje bezpośredni dostęp z sieci Internet. Są one bowiem bardziej podatne na ataki, które skutkować mogą kradzieżą danych.

Szyfrowanie baz danych

Szyfrowanie danych chroni je w sytuacji, w której weszły one w posiadanie niepowołanych osób. Ponadto zmniejsza ryzyko potencjalnych ataków, bowiem w pełni zaszyfrowane bazy danych są dla złodziei całkowicie bezużyteczne.

Jednym z mechanizmów szyfrowania całych baz danych jest *TDE* (ang. *Transparent Data Encryption*). Metoda ta operuje na danych w spoczynku (ang. *data at rest*), czyli takich, które nie są aktualnie edytowane czy przesyłane przez sieć. Ważnym atrybutem *TDE* jest przezroczystość – oznacza ona, że aplikacje korzystające z zaszyfrowanych tą metodą baz danych nie muszą być w żaden sposób dostosowywane.

Kolejną metodą ochrony danych jest szyfrowanie wybranych kolumn w tabelach. Jej istotną zaletą jest możliwość używania osobnego klucza kryptograficznego dla każdej z szyfrowanych kolumn. Zwiększa to trudność przeprowadzania ataków wykorzystujących *tęczowe tablice* (ang. *rainbow tables*). Wadą jest natomiast zmniejszona wydajność – odszyfrowanie każdej kolumny osobnym kluczem zajmuje więcej czasu niż całej bazy danych za jednym razem, przy użyciu jednego klucza kryptograficznego.

Można także szyfrować cały dysk maszyny, na której zlokalizowana jest baza danych. Zapewnia to większe bezpieczeństwo od szyfrowania wyłącznie samej bazy.

Użytkownicy baz danych

Do baz danych powinny mieć dostęp wyłącznie zaufane osoby, dla których jest on niezbędny do realizacji powierzonych im zadań. Powinny one posiadać minimum uprawnień pozwalających na ich wykonywanie. W wyjątkowych przypadkach, kiedy potrzebne są wyższe uprawnienia, należy używać klauzuli takich jak *EXECUTE AS* zamiast przydzielać je na stałe. Polityka bezpieczeństwa powinna wymuszać na użytkownikach wybieranie silnych haseł oraz ich regularne zmiany.

Bezpieczeństwo sieciowe

Firewall na serwerze bazy danych powinien domyślnie odrzucać wszystkie połączenia poza tymi, które inicjowane są przez upoważnione aplikacje czy inne serwery.

Dane trafiające do i z bazy powinny być przesyłane przy użyciu bezpiecznych protokołów komunikacyjnych, aby zabezpieczyć je na wypadek podsłuchiwania ruchu sieciowego. Jeżeli ruch odbywa się wyłącznie z kontrolowanej sieci lokalnej, można wykorzystać nieszyfrowane protokoły.

Web Application Firewall

Web Application Firewall to oprogramowanie przeznaczone do ochrony aplikacji webowych. Monitoruje wychodzący i przychodzący ruch sieciowy, wykrywając i zapobiegając atakom takim jak *SQL Injection* czy *cross-site scripting*. Dzięki temu zagrożenia niwelowane są jeszcze zanim dotrą do bazy danych.

Aktualizacja systemu bazodanowego

Nieaktualny system zarządzania bazą danych może być podatny na ataki, które nie byłyby możliwe po jego aktualizacji. Należy zatem dbać o to, by wersja używanego oprogramowania była możliwie jak najwyższa (pomijając niestabilne wydania).

Logowanie i audytowanie

Czynności wykonywane przez użytkowników bazy danych powinny być logowane i regularnie monitorowane w celu wykrywania niedozwolonych zachowań.

Ponadto, należy przeprowadzać audyty bezpieczeństwa mające na celu wykrywanie istniejących podatności na zagrożenia.