41 Zasady zabezpieczania serwera baz danych

EFEKTY KSZTAŁCENIA Z PODSTAWY PROGRAMOWEJ:

- **PKZ(E.b)(13) stosuje programy komputerowe wspomagające wykonywanie zadań;**
- **E.13.2(8) dobiera sposoby ustawiania zabezpieczeń dostępu do danych;**
- **E.13.2(9) zarządza bazą danych i jej bezpieczeństwem;**
- **E.13.2(10) określa uprawnienia poszczególnych użytkowników i zabezpieczenia dla nich;**
- **E.13.2(12) zarządza kopiami zapasowymi baz danych i ich odzyskiwaniem;**
- **E.13.2(14) dokonuje naprawy baz danych.**

W TYM ROZDZIALE:

- **przypomnisz sobie, jakie są typy ataków na bazy danych;**
- **dowiesz się, na czym polega zapewnienie ciągłości pracy bazy danych;**
- **poznasz zasady właściwej polityki poufności podczas administrowania bazą danych;**
- **przypomnisz sobie, co to jest schemat bazy danych;**
- **poznasz zasady tworzenia i usuwania schematów;**
- **dowiesz się, jakie są zasady administrowania uprawnieniami w bazie danych;**
- **nauczysz się naprawiać bazę danych;**
- **nauczysz się tworzyć kopie zapasowe bazy danych i odzyskiwać dane z kopii.**

Wprowadzenie

Zagrożenia dla baz danych mogą wynikać z działań człowieka, awarii sprzętu, oprogramowania, braku zasilania lub niewłaściwych zabezpieczeń systemów informatycznych. Ataki na bazy danych mogą mieć na celu odczytanie chronionych informacji, ich modyfikację lub zniszczenie. Administrator baz danych ma obowiązek odpowiednio zabezpieczyć dane podlegające ochronie ustawowej, np. dane osobowe, utwory objęte prawami autorskimi. Ataki można podzielić na dwie grupy:

- **pasywne** – polegają na podglądaniu lub prowadzeniu nasłuchu sieciowego, np. podglądanie hasła wpisywanego na klawiaturze, nagrywanie wpisywania hasła kamerą, używanie urządzeń lub programów typu keylogger, prowadzenie nasłuchu w sieciach radiowych, przechwytywanie e-maili lub plików, analizowanie ruchu sieciowego;
- **aktywne** – wiążą się z modyfikacją danych i ingerencją atakującego w obrębie sieci lub systemu informatycznego, np. podszywanie się pod osobę, komputer lub urządzenie uprzywilejowane, posłużenie się danymi przechwyconymi w sposób pasywny i na tej podstawie uzyskanie dostępu do określonych zasobów, zmiana fragmentu oryginalnego komunikatu lub jego opóźnianie, blokowanie działania usług przez przeciążenia, przeładowania, zagłuszanie lub zniszczenie medium transmisyjnego.

Elementem zabezpieczenia systemu jest zapewnienie mu **ciągłości pracy**, np. zastosowanie systemu zasilaczy awaryjnych i agregatów prądotwórczych czy systemu kopii zapasowych.

Polityka bezpieczeństwa wymaga określenia kontroli dostępu do SZBD i do danych. Do najważniejszych zadań należy określenie:

- **dostępności** – użytkownik powinien mieć dostęp tylko do danych dla niego przeznaczonych;
- **spójności** – na każdego z użytkowników są nałożone ograniczenia dotyczące modyfikacji danych, do których nie powinien mieć dostępu (np. zmiany hasła lub usunięcia konta administratora bazy);
- **poufności** – użytkownik nie będzie mógł podglądać danych przechowywanych przez innych użytkowników i tych, do których nie powinien mieć dostępu.

Podstawowym sposobem ochrony danych jest zapewnienie fizycznej ochrony serwerów oraz wprowadzenie ograniczeń na wykonanie operacji na obiektach bazy danych. Przyznawanie uprawnień jest realizowane za pomocą klauzuli **GRANT**, a odebranie – za pomocą klauzuli **REVOKE**. Aby ułatwić zarządzanie uprawnieniami definiuje się **role** – zestaw uprawnień i ograniczeń (brak uprawnień) określony dla grupy użytkowników.

Kontrola dostępu bazująca na **modelu Bell-La Padula** polega na przypisywaniu elementom stopni kategorii bezpieczeństwa: Top secret>Secret>Confidential>Restricted>Unclassified, natomiast podmiotom – określonych poziomów uprawnień. Zezwala się na odczyt informacji tylko w dół – podmiot uzyskuje prawo do odczytu

obiektu tylko wtedy, gdy jego poziom uprawnień jest większy lub równy poziomowi obiektu. Przepływ informacji jest możliwy tylko do góry – podmiot może pisać do obiektu tylko wtedy, gdy poziom uprawnień podmiotu jest mniejszy bądź równy poziomowi uprawnień obiektu oraz podmiot ma prawo zapisu do obiektu (podmioty nie mogą zapisać informacji do obiektów na niższych poziomach). Podmiot z przypisanym poziomem uprawnień nie może komunikować się z podmiotem, który nie ma przypisanego poziomu uprawnień.

Schemat bazy danych to struktura, w której znajdują się obiekty bazy danych, takie jak: domeny, tabele, widoki, funkcje, typy danych. Schematy nie mogą być zagnieżdżone (nie może wystąpić schemat wewnątrz innego schematu). Schemat jest przestrzenią nazw. Można używać tej samej nazwy obiektu w różnych schematach, jednak nazwę należy poprzedzić nazwą schematu i znakiem kropki. Jeśli podczas tworzenia obiektu nie zostanie określony schemat, do którego dany obiekt powinien należeć, wówczas obiekt jest umieszczany w domyślnym schemacie **public**. Dostęp do obiektu w schemacie może uzyskać użytkownik posiadający odpowiednie uprawnienia. Użytkownik może wprowadzać zmiany w schematach, do których ma uprawnienia. Aby utworzyć schemat, używa się polecenia CREATE SCHEMA schemat. Aby usunąć schemat, używa się polecenia DROP SCHEMA schemat. Jeśli schemat nie jest pusty i zawiera obiekty, np. tabele, należy użyć usuwania kaskadowego DROP SCHEMA schemat CASCADE.

Podczas pracy z bazami danych może dojść do uszkodzenia tabel baz danych. Naprawa uszkodzeń polega na uruchomieniu programu służącego do naprawy bazy danych lub odtworzeniu bazy z kopii zapasowej. Dla bazy MySQL naprawę tabel można przeprowadzić za pomocą narzędzia phpMyAdmin lub za pomocą polecenia **mysqlcheck** wykonywanego z linii poleceń – konsoli systemu operacyjnego.

Jednym z elementów systemu zapewnienia bezpieczeństwa bazy powinno być regularne tworzenie kopii zapasowych bazy danych i planowanie procedur przywracania danych. Wykonywanie kopii bezpieczeństwa i testowanie procedur ich przywracania jest obowiązkiem administratora bazy danych. Kopie zapasowe w bazie PostgreSQL można wykonać za pomocą narzędzi wiersza poleceń systemu operacyjnego, np.

- **pg_dump** – pozwala na stworzenie kopii wybranej bazy;
- **pg_dumpall** – pozwala na stworzenie kopii wszystkich baz;
- **pg_restore** – pozwala na odtworzenie danych kopii.

Kopie zapasowe MySQL można tworzyć za pomocą narzędzia konsoli systemowej **mysqldump**, a odtworzenie bazy danych wykonuje się za pomocą polecenia: mysql --user=root --password=Qwerty123 nazwa_bazy < nazwa_pliku.sql.

Kopie zapasowe można również wykonywać i odtwarzać dzięki narzędziom graficznym, np. phpMyAdmin lub MySQL Workbench dla MySQL, lub za pomocą narzędzia pgAdmin III dla PostgreSQL.

LITERATURA

- P. Domka, *Bazy danych i systemy baz danych*, WSiP, Warszawa 2013:
  - rozdział 39, s. 300 – *Podział zagrożeń dla bazy danych i sposoby przeciwdziałania im*;
  - rozdział 40, s. 303 – *Zabezpieczenia dostępu do danych (zarządzanie bezpieczeństwem)*;
  - rozdział 41, s. 308 – *Schematy*;
  - rozdział 42, s. 310 – *Nadawanie i odbieranie uprawnień PostgreSQL*;
  - rozdział 43, s. 315 – *Kopia zapasowa i odtwarzanie bazy danych*.

NOTATKI

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

ZADANIE 1.

Opisz swoimi słowami różnice między atakami pasywnymi i aktywnymi. Podaj przykłady programów, które mogą być wykorzystane do przeprowadzenia ataków. Odpowiedź zapisz w edytorze tekstu. Zapisz dokument.

ZADANIE 2.

Wyszukaj w internecie informacje o elementach, z których powinna się składać polityka bezpieczeństwa firmy. Opisz w kilku zdaniach trzy wybrane składniki polityki bezpieczeństwa. W edytorze tekstu wpisz odpowiednie informacje zgodnie z poniższą formatką. Zapisz dokument.

Nazwa składnika	Opis składnika

ZADANIE 3.

Skorzystaj z narzędzia mysqlcheck i sprawdź, czy w tabelach przykładowej bazy, np. firma, nie występują błędy. W edytorze tekstu wpisz odpowiednie informacje zgodnie z poniższą formatką. Zapisz dokument.

Nazwa tabeli	Użyte polecenie	Wynik testu
Zrzut ekranu potwierdzający wykonanie zadania		

ZADANIE 4.

Skorzystaj z narzędzia pg_dump i sporządź kopie zapasowe tabel z wybranej bazy danych, np. firma. W edytorze tekstu wpisz odpowiednie informacje zgodnie z poniższą formatką. Zapisz dokument.

Nazwa tabeli	Użyte polecenie	Nazwa pliku kopii zapasowej	Rozmiar pliku kopii zapasowej
Zrzut ekranu potwierdzający wykonanie zadania			

ZADANIE 5.

Skorzystaj z narzędzia pg_restore, odtwórz dane z kopii stworzonych w zadaniu 4. W edytorze tekstu wpisz odpowiednie informacje zgodnie z poniższą formatką. Zapisz dokument.

Nazwa tabeli	Użyte polecenie	Nazwa pliku kopii zapasowej	Odtwarzanie zakończone sukcesem
Zrzut ekranu potwierdzający wykonanie zadania			

Rozwiązania zadań zapisz w pliku pod nazwą BD_41_nazwisko.doc. Przedstaw do oceny nauczycielowi.

PODSUMOWANIE

TEST 41. Część pisemna egzaminu zawodowego

Zadanie 1.
Które ataki wiążą się z modyfikacją danych i ingerencją atakującego w obrębie sieci lub systemu informatycznego?
A. Pasywne. B. Aktywne. C. Sieciowe. D. Inżynierii społecznej.

Zadanie 2.
Program typu sniffer zwykle jest wykorzystywany w atakach
A. pasywnych.
B. aktywnych.
C. DoS.
D. typu blokada działania.

Zadanie 3.
Odebranie uprawnień jest realizowane za pomocą klauzuli
A. GRANT. B. REVOKE. C. ADD. D. REMOVE.

Zadanie 4.
Które zdanie, dotyczące kontroli dostępu bazującej na modelu Bell-La Padula, jest prawdziwe?
A. Podmiot uzyskuje prawo do odczytu obiektu tylko wtedy, gdy jego poziom uprawnień jest mniejszy lub równy poziomowi uprawnień obiektu.
B. Podmiot uzyskuje prawo do odczytu obiektu tylko wtedy, gdy jego poziom uprawnień jest mniejszy od poziomu uprawnień obiektu.
C. Podmiot uzyskuje prawo do odczytu obiektu tylko wtedy, gdy jego poziom uprawnień jest większy lub równy poziomowi uprawnień obiektu.
D. Podmiot uzyskuje prawo do odczytu obiektu tylko wtedy, gdy jego poziom uprawnień jest większy od poziomu uprawnień obiektu.

Zadanie 5.
Kopie zapasowe MySQL można tworzyć za pomocą narzędzia konsoli systemowej
A. backup.exe.
B. mysqldump.
C. Mysql.
D. mysqlbackup.

ZADANIE EGZAMINACYJNE 1. Część praktyczna egzaminu zawodowego

Jesteś pracownikiem firmy zajmującej się tworzeniem oprogramowania, projektowaniem i wdrażaniem systemów baz danych. Do firmy zgłosił się klient, który przypuszcza, że w jego bazie danych mogą występować błędy. Klient posiada bazę danych **firma** w systemie MySQL, ale nie potrafi powiedzieć, jakie tabele są w niej utworzone. Ponadto klient chciałby, aby została utworzona kopia zapasowa bazy.

Twoim zadaniem jest:
- nawiązanie połączenia z bazą danych;
- wybranie bazy danych **firma**;
- wyświetlenie nazw wszystkich tabel;
- sprawdzenie, czy w poszczególnych tabelach nie występują błędy;
- sporządzenie kopii zapasowej bazy **firma**;
- sprawdzenie możliwości odtworzenia danych z kopii zapasowej.

Wykonaj wszystkie polecenia na stanowisku wyposażonym w serwer baz danych z zainstalowaną bazą danych **firma** w systemie MySQL.

Rezultaty podlegające ocenie:
- nawiązanie połączenia z bazą danych;
- wybranie bazy danych **firma**;
- wyświetlenie nazw wszystkich tabel;
- sprawdzenie, czy w poszczególnych tabelach nie występują błędy;
- sporządzenie kopii zapasowej bazy **firma**;
- sprawdzenie możliwości odtworzenia danych z kopii zapasowej;
- przebieg prac zgodny z zasadami BHP, ergonomii i organizacji pracy.

Czas przeznaczony na wykonanie zadania wynosi 60 minut.

PODSUMOWANIE

ZADANIE EGZAMINACYJNE 2. Część praktyczna egzaminu zawodowego

Jesteś pracownikiem firmy zajmującej się tworzeniem oprogramowania, projektowaniem i wdrażaniem systemów baz danych. Do firmy zgłosił się klient, którego baza danych **biblioteka** powinna składać się z tabel:

- **czytelnicy**:
  - id_czytelnika – klucz główny;
  - nazwisko;
  - imie;
  - adres;
- **ksiazki**:
  - id_ksiazki, – klucz główny;
  - tytul;
  - autor;
  - rok_wydania;
  - wydawnictwo;
- **wypozyczenia**:
  - id_wypozyczenia – klucz główny;
  - data_wypozyczenia;
  - id_czytelnika – klucz obcy z tabeli czytelnicy;
  - id_ksiazki – klucz obcy z tabeli ksiazki.

Dla zwiększenia bezpieczeństwa klient chciałby, aby uprawnienia pracowników zostały ograniczone do niezbędnego minimum. Wykaz uprawnień został przedstawiony w tabeli 2.41.1.

Tabela 2.41.1. Wykaz uprawnień

	Tabele		
Konta	**czytelnicy**	**ksiazki**	**wypozyczenia**
Nowak	SELECT, INSERT, DELETE, UPDATE	SELECT	SELECT
Kowalski	SELECT	SELECT, INSERT, DELETE, UPDATE	SELECT
Iksinski	SELECT	SELECT	SELECT, INSERT, DELETE, UPDATE
Administrator	ALL	ALL	ALL

Twoim zadaniem jest:

- nawiązanie połączenia z bazą danych;
- utworzenie bazy danych **biblioteka**;
- utworzenie tabel **czytelnicy**, **ksiazki** i **wypozyczenia**;
- utworzenie kont **Nowak**, **Kowalski**, **Iksinski**, **Administrator**;
- przydzielenie odpowiednich uprawnień do tabel;
- wprowadzenie do każdej tabeli dwóch przykładowych rekordów;
- utworzenie na pulpicie pliku **konta.txt** zawierającego hasła utworzonych użytkowników.

Wykonaj wszystkie polecenia na stanowisku wyposażonym w serwer baz danych z zainstalowaną bazą danych MySQL i PostgerSQL.

Rezultaty podlegające ocenie:

- nawiązanie połączenia z bazą danych;
- utworzenie bazy danych **biblioteka**;
- utworzenie tabel: **czytelnicy**, **ksiazki** i **wypozyczenia**;
- utworzenie kont: **Nowak**, **Kowalski**, **Iksinski**, **Administrator**;
- przydzielenie odpowiednich uprawnień do tabel;
- wprowadzenie do każdej tabeli dwóch przykładowych rekordów;
- utworzenie na pulpicie pliku **konta.txt** zawierającego hasła utworzonych użytkowników;
- przebieg prac zgodny z zasadami BHP, ergonomii i organizacji pracy.

Czas przeznaczony na wykonanie zadania wynosi 60 minut.