TEMAT 18

# Użytkownicy, role i mechanizmy uwierzytelniania

## Kto łączy się z bazą i dlaczego nie każdy może robić wszystko

**Teoria • przykład • schemat • pytanie • ćwiczenie**

Bazy danych • 45 minut • bez komputerów

# Cel lekcji i pytanie na start

| | |
|---|---|
| CEL | Rozróżnisz użytkownika, rolę, uwierzytelnianie i autoryzację. |
| ZROZUMIESZ | Dlaczego jedno wspólne konto dla całej szkoły stanowi zagrożenie. |
| ODCZYTASZ | Tabelę kont, ról i uprawnień oraz przewidzisz wynik polecenia SQL. |
| ROZPOZNASZ | Błąd logowania, brak uprawnienia i zbyt szeroki dostęp. |

**Pytanie: czy znajomość hasła oznacza prawo do usuwania rekordów?**

# Cztery pojęcia, których nie mylimy

| POJĘCIE | PROSTE WYJAŚNIENIE | PYTANIE KONTROLNE |
|---|---|---|
| użytkownik | konto osoby lub programu | kto próbuje wejść? |
| rola | zestaw wspólnych uprawnień | jaką funkcję pełni? |
| uwierzytelnianie | potwierdzenie tożsamości | czy to naprawdę ta osoba? |
| autoryzacja | sprawdzenie dozwolonych działań | co wolno jej zrobić? |

**Najpierw system potwierdza tożsamość. Dopiero potem sprawdza zakres dostępu.**

# Prosty przykład: szkolna baza danych

| KONTO | ROLA | POTRZEBA | DOZWOLONE |
|---|---|---|---|
| anna | sekretariat | poprawia dane uczniów | SELECT, UPDATE |
| jan | nauczyciel | odczytuje uczniów i wpisuje oceny | SELECT, INSERT |
| ewa | dyrektor | czyta raporty | SELECT |
| backup_app | kopia zapasowa | wykonuje zaplanowany backup | BACKUP |

**Konto identyfikuje użytkownika. Rola opisuje jego zadanie. Uprawnienie określa konkretną operację.**

# Schemat logowania i dostępu

1

## Identyfikacja

Użytkownik podaje nazwę konta.

2

## Uwierzytelnienie

Serwer sprawdza hasło, certyfikat lub inny dowód.

3

## Odczyt roli

Serwer ustala, do jakich ról należy konto.

4

## Autoryzacja

Serwer porównuje polecenie z uprawnieniami.

**Poprawne hasło otwiera drogę do konta, ale zakres działań nadal ograniczają role i uprawnienia.**

# Uwierzytelnianie: jak potwierdzamy tożsamość

| MECHANIZM | CO SPRAWDZA SYSTEM | PRZYKŁAD |
|---|---|---|
| hasło | sekret znany użytkownikowi | login + hasło |
| certyfikat | ważny cyfrowy dokument | certyfikat klienta |
| konto systemowe | tożsamość z systemu lub domeny | Windows / Active Directory |
| wiele składników | więcej niż jeden dowód | hasło + kod |

**Szczegóły zależą od SZBD i konfiguracji serwera. Hasła nie zapisujemy w tabeli uczniów ani w kodzie programu.**

# Rola porządkuje uprawnienia

**KONTA**

anna
ola
piotr

**ROLA: NAUCZYCIEL**

SELECT uczniowie
INSERT oceny

**TABELE**

UCZNIOWIE
OCENY

**Zmiana uprawnień roli działa dla wszystkich kont przypisanych do tej roli.**

# Użytkownicy i role a tabele biznesowe

## KONTA I ROLE

Służą do zarządzania dostępem do systemu bazy danych.

## TABELA UCZNIOWIE

Przechowuje rekordy opisujące uczniów i ich atrybuty.

**konto: anna ≠ rekord: uczen_id = 17**

**Konto bazy i rekord w tabeli mogą dotyczyć tej samej osoby, ale pełnią inne funkcje.**

# Tworzenie konta lub roli w SQL

```
-- Przykład składni PostgreSQL
CREATE USER anna WITH PASSWORD '***';
CREATE ROLE nauczyciel;
GRANT nauczyciel TO anna;
```

CREATE USER tworzy konto mogące się logować. CREATE ROLE tworzy rolę. GRANT przypisuje rolę do konta.

Składnia różni się między PostgreSQL, MySQL/MariaDB, SQL Server i Oracle.

# Uprawnienia do tabeli

```
-- Rola może odczytać tabelę uczniowie
GRANT SELECT ON uczniowie TO nauczyciel;

-- Rola może dopisywać oceny
GRANT INSERT ON oceny TO nauczyciel;
```

**SELECT pozwala czytać rekordy. INSERT pozwala dodawać rekordy. UPDATE zmienia dane, a DELETE je usuwa.**

**Pytanie: czy nauczyciel potrzebuje DELETE na tabeli uczniowie?**

# Co się stanie po wykonaniu zapytania

| UŻYTKOWNIK | ROLA | POLECENIE | WYNIK |
|---|---|---|---|
| anna | sekretariat | SELECT * FROM uczniowie | wykonane |
| jan | nauczyciel | INSERT INTO oceny ... | wykonane |
| jan | nauczyciel | DELETE FROM uczniowie ... | odrzucone |
| ewa | raporty | UPDATE uczniowie ... | odrzucone |

**Serwer najpierw rozpoznaje konto i role, a potem porównuje polecenie z nadanymi uprawnieniami.**

# Przewidywanie wyniku zapytania

**Rola czytelnik ma wyłącznie uprawnienie SELECT do tabeli UCZNIOWIE.**

```
UPDATE uczniowie
SET nazwisko = 'Nowak'
WHERE uczen_id = 17;
```

**Wynik: serwer odrzuci polecenie. Warunek WHERE może być poprawny, ale rola nie ma uprawnienia UPDATE.**

# Najczęstsze błędy i zagrożenia

| BŁĄD | SKUTEK | POPRAWNE DZIAŁANIE |
|---|---|---|
| wspólne konto dla wszystkich | brak odpowiedzialności za operacje | osobne konta |
| hasło zapisane w notatniku | łatwe przejęcie dostępu | bezpieczne przechowywanie |
| rola ma DELETE „na zapas” | ryzyko utraty rekordów | minimalne uprawnienia |
| konto byłego pracownika aktywne | niepotrzebna możliwość logowania | wyłączenie konta |
| konto aplikacji jak administrator | duży skutek włamania | osobna rola aplikacji |

**Bezpieczeństwo dostępu zależy od poprawnej konfiguracji i codziennych nawyków użytkowników.**

# Rozpoznaj rodzaj problemu

| KOMUNIKAT / SYTUACJA | RODZAJ PROBLEMU | CO SPRAWDZIĆ |
|---|---|---|
| password authentication failed | uwierzytelnianie | login, hasło, metodę logowania |
| permission denied for table uczniowie | autoryzacja | rolę i uprawnienia |
| role nauczyciel does not exist | konfiguracja ról | nazwę roli |
| syntax error near WHERE | składnia SQL | budowę zapytania |
| foreign key violation | relacje danych | czy wskazany rekord istnieje |

**Nie każdy błąd podczas pracy z bazą oznacza błędne hasło.**

# Zasada najmniejszych uprawnień

| SEKRETARIAT | NAUCZYCIEL | RAPORTY |
| --- | --- | --- |
| SELECT, INSERT, UPDATE na danych uczniów | SELECT uczniów<br>INSERT, UPDATE ocen | SELECT<br>bez zmiany danych |

**Każda rola otrzymuje tylko prawa potrzebne do wykonania konkretnego zadania.**

**Pytanie: które konto powinno mieć prawo tworzenia nowych użytkowników?**

# Ćwiczenie na kartce: dobierz role

**Sytuacja**

Projektujesz dostęp do tabel UCZNIOWIE, OCENY i RAPORTY.

| OSOBA | ZADANIE | TWOJA ROLA I PRAWA |
|---|---|---|
| sekretarka | poprawia adres ucznia | ..... |
| nauczyciel | wpisuje oceny swojej klasy | ..... |
| dyrektor | czyta zestawienia | ..... |
| administrator | tworzy konta i role | ..... |

**Dodatkowo: zaznacz jedno uprawnienie, którego dana osoba nie powinna otrzymać.**

# Omówienie ćwiczenia

| | |
|---|---|
| **SEKRETARIAT** | SELECT i UPDATE na danych uczniów. Bez prawa do zmiany ocen. |
| **NAUCZYCIEL** | SELECT uczniów oraz INSERT i UPDATE ocen. Bez usuwania uczniów. |
| **DYREKTOR** | SELECT do raportów. Brak potrzeby codziennej zmiany rekordów. |
| **ADMINISTRATOR** | Zarządza kontami i rolami. Konta administracyjnego nie używa do zwykłej pracy. |

**Dobra odpowiedź łączy zadanie pracownika z minimalnym, uzasadnionym zakresem uprawnień.**

# Podsumowanie i bilet wyjścia

| | |
|---|---|
| **UŻYTKOWNIK** | Konto osoby albo programu łączącego się z bazą. |
| **ROLA** | Wspólny zestaw uprawnień przypisywany kontom. |
| **UWIERZYTELNIANIE** | Potwierdza tożsamość użytkownika. |
| **AUTORYZACJA** | Sprawdza, czy użytkownik może wykonać polecenie. |

**BILET WYJŚCIA: wyjaśnij różnicę między uwierzytelnianiem a autoryzacją i podaj przykład z tabelą OCENY.**