
Bezpieczeństwo baz danych

— Monika Badełek —

Plan referatu

- Dlaczego warto dbać o bezpieczeństwo naszej bazy danych?
- Czym jest bezpieczeństwo baz danych?
- Trzy główne aspekty bezpieczeństwa baz danych.
- Przykładowe metody ochrony bazy danych.

Podstawowe informacje

Baza danych - Zbiór informacji przechowywanych w komputerze.

Bezpieczeństwo - bycie wolnym od zagrożeń

Bezpieczeństwo bazy danych - mechanizm polegający na zabezpieczeniu bazy danych przed celowym bądź przypadkowym zagrożeniem ze strony użytkowników

Dlaczego musimy dbać o bazę danych? 1.0

W obecnych czasach dążymy do bezpieczeństwa każdego z naszych cennych urządzeń - komputera, smartfonu czy samochodu.

Dlaczego więc nie dbać o **bazę danych**?

Jest wiele powodów by to robić...



Dlaczego musimy dbać o bazę danych? 2.0

1. Wrażliwe dane podawane w portalach internetowych
 - a. Dane z kart kredytowych (np. na Allegro)
 - b. Numery dowodu osobistego lub PESEL (np. podczas rezerwowania biletu lotniczego)
 - c. Adresy zamieszkania (to już praktycznie wszędzie)

W przypadku posiadania tego typu danych złodziej w łatwy sposób może zaciągnąć na nas kredyt, podszyć się pod nas w innym portalu internetowym lub zaszkodzić nam na tysiące innych sposobów.

Przykłady: W 2016 roku z baz danych polskich kancelarii wyciekło ponad 800 tysięcy numerów pesel i innych danych osobowych.

Źródło: antyweb.pl/pesel-wyciek-danych/

Co to znaczy dbać o bazę danych?

Typowy przebieg informacji
w systemie bazodanowym:

Należy zadbać o bezpieczeństwo
każdego z tych kroków.



Trzy złote zasady bezpieczeństwa bazy danych

1. Tajność
2. Integralność
3. Dostępność



Tajność (secrecy)

Jest to chronienie bazy danych przed **autoryzowanymi** użytkownikami.

Poleca na tym, że trzeba zapewnić, że użytkownik ma prawo do czynności, którą właśnie próbuje wykonać.

Przykład:

- Gość portalu z zakupami nie powinien mieć dostępu do dokładnych danych o stanie magazynów czy umieszczonych w bazie danych faktur.

Integralność

Zapewnia ochronę bazy danych przez autoryzowanymi użytkownikami.

Ma na celu zapewnić, że działanie które chce wykonać użytkownik jest zgodne z jego uprawnieniami.

Przykład:

- Pracownik firmy powinien mieć możliwość edytowania swoich danych, jednak nie powinien móc edytować danych innych pracowników.

Jak zapewniamy tajność i integralność?

1. Szyfrowanie danych - tylko autoryzowani użytkownicy mogą je odczytać.
2. Nadawanie specjalnych praw dostępu dla użytkowników.
3. Korzystanie z tzw. widoków (patrz: SQL).
4. Autentykacja i autoryzacja użytkowników bazy danych.

Dostępność

Chodzi tu o fizyczne własności bazy danych, takie jak np. minimalizacja awaryjności całego systemu. Do tego możemy zaliczyć:

- Wykonywanie regularnych back-upów systemu.
- Regularny przegląd sprzętu komputerowego.
- Ograniczenie liczby jednoczesnych połączeń z bazą danych.
- Zapewnienie odpowiedniej przestrzeni dyskowej.

Dziękuję za uwagę!