

Bezpieczeństwo bazy danych PostgreSQL

Hubert „depez” Lubaczewski

luty 2003

Co to jest bezpieczeństwo baz danych?

Czego na pewno nie zaliczamy do BBD?

- SQL injection
- włamania (ftpd/whatever-d) na serwer BD

Co to jest bezpieczeństwo BD? (c.d.)

Co zaliczamy do BBD?

- kradzież danych
- zniszczenie danych
- modyfikacja danych

Metody osiągnięcia BDD

- hardware
 - UPS?
- software — OS
 - szyfrowanie dysków

Metody osiągnięcia BBD (c.d.)

- software — serwer SQL
 - struktura danych w PostgreSQL (database/schema/tables/
views/functions/rules/...)
 - konta użytkowników
 - blokowanie dostępu do bazy (pg_hba)
 - zarządzanie uprawnieniami — grant/revoke
 - funkcje i widoki — SECURITY DEFINED (function)
 - szyfrowanie rekordów

Kiedy i jak powinniśmy się zabezpieczać?

- wartość danych
 - wartość bezpośrednia
 - wartość pośrednia
- zarządzanie ryzykiem
 - kiedy wartość danych jest wyższa od kosztu zabezpieczenia
 - kiedy wartość danych jest niższa od kosztu zabezpieczenia

Czy można zabezpieczyć się całkowicie?

- Dlaczego tak?
 - szyfrowanie
 - konta
 - funkcje
 - widoki
 - szyfrowanie partycji

Czy można zabezpieczyć się całkowicie? (c.d.)

- Dlaczego nie?
 - za dużo zachodu
 - spowolnienie
 - komplikacje w sytuacjach awaryjnych