BANKA SLOVENIJE
EVROSISTEM

NADZOR DOSTOPA DO PODATKOV NA NIVOJU POSAMEZNIH ZAPISOV

Miha Peternel

Banka Slovenije

Uvod

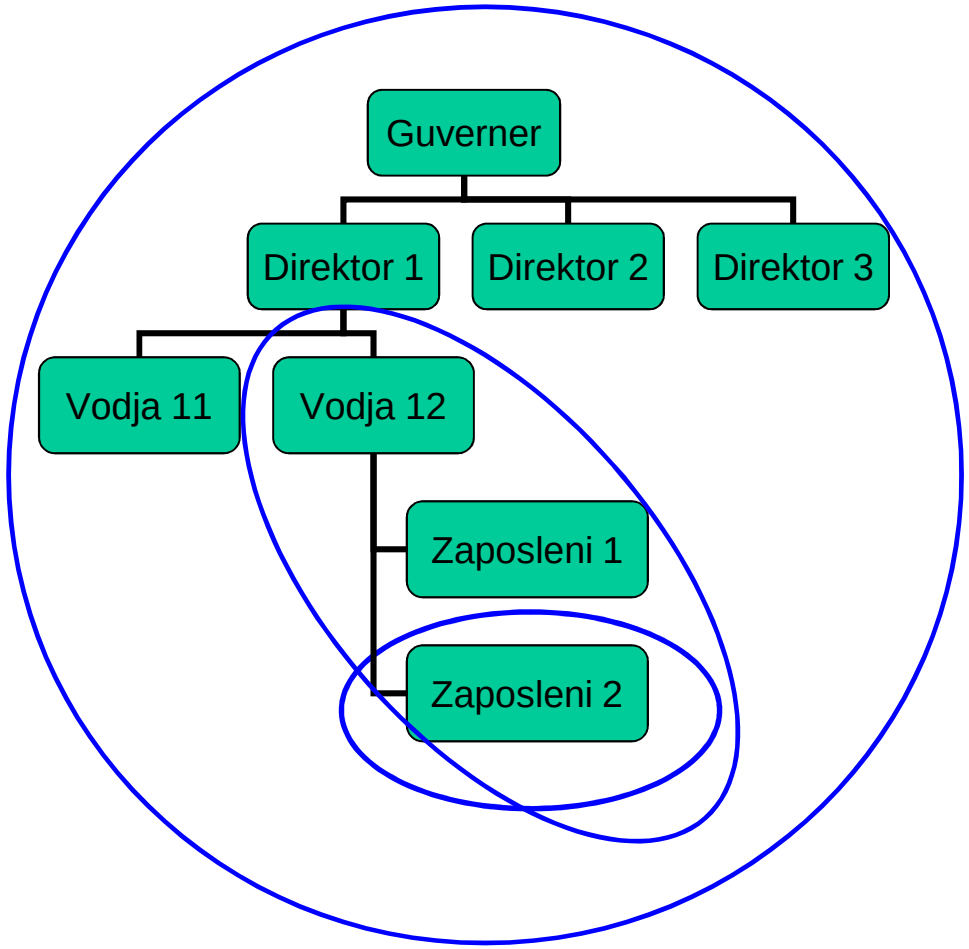
BANKA SLOVENIJE
EVROSISTEM

- Aplikacija za interno uporabo
- Tehnologija v skladu z internimi standardi
  - Baza Oracle
  - Uporabniški vmesnik Oracle Forms

Poslovna zahteva

BANKA SLOVENIJE
EVROSISTEM

- Vsak uporabnik ima dostop samo do zapisov, ki se nanašajo nanj ali na njegove podrejene



Dodeljevanje pravic na nivoju objektov

BANKA SLOVENIJE
EVROSISTEM

- Če uporabniku dodelimo dostop do tabele, potem ima dostop do vseh zapisov v njej
- Dostop do posameznih zapisov lahko nadziramo v posameznih modulih uporabniškega vmesnika
  - Kontrole moramo vgraditi v vsak modul posebej
  - Dostop do podatkov preko ODBC ali SQL*Plus se izogne tem kontrolam

Namišljena privatna podatkovna baza

BANKA SLOVENIJE
EVROSISTEM

- Od Oracle 8i dalje
- Vsakemu SQL stavku pred izvajanjem doda selekcijski pogoj, ki ustreza varnostnim zahtevam

Namišljena privatna podatkovna baza - izvedba

BANKA SLOVENIJE
EVROSISTEM

- Definirati moramo:
  - Varnostno funkcijo, ki vrne selekcijski pogoj
  - Varnostno politiko na tabeli
    - Politika pred izvedbo vsakega SQL stavka pokliče varnostno funkcijo in v selekcijski pogoj doda niz, ki ga vrne varnostna funkcija

Namišljena privatna podatkovna baza - primer

BANKA SLOVENIJE
EVROSISTEM

Ime	Nadrejeni
Jože	
Andreja	Jože
Vlado	Jože

SELECT ime FROM zaposleni;

Jože

Rezultat varnostne funkcije:
`1=1`

```
SELECT ime
FROM zaposleni
WHERE 1=1;
```

```
Ime
------
Jože
Andreja
Vlado
```

Vlado

Rezultat varnostne funkcije:
`ime = 'Vlado'`

```
SELECT ime
FROM zaposleni
WHERE ime = 'Vlado';
```

```
Ime
------
Vlado
```

Prednosti namišljene privatne podatkovne baze

BANKA SLOVENIJE
EVROSISTEM

- Varnostne zahteve izpolnimo na nivoju podatkovne baze, zato se pri razvoju uporabniškega vmesnika z njimi ni treba ukvarjati
- Varnostne zahteve so izpolnjene ne glede na način dostopa do baze

Težave - Sintaktične napake

BANKA SLOVENIJE
EVROSISTEM

- Težava
  - Selekcijski pogoji se sestavljajo med izvajanjem, zato lahko nastane sintaktično nepravilen SQL stavek
- Rešitev
  - Dobro testiranje
  - Dobro logiranje

Težave - Neskladna poročila

BANKA SLOVENIJE
EVROSISTEM

- Težava
  - Direktor in zaposleni z dna hierarhije poženeta isto poročilo in dobita različne rezultate
- Rešitev
  - Na poročilu mora biti jasno označeno, kadar zaradi varnostne politike niso prikazani vsi zapisi

Težave - Različne zahteve za vpogled in spreminjanje

BANKA SLOVENIJE
EVROSISTEM

- Težava
  - Različne zahteve za vpogled in spreminjanje podatkov
- Rešitev
  - Na tabeli definiramo dve politiki. Ena velja za vpogled, druga za spreminjanje podatkov

Težave - Vpogled v vse zapise

BANKA SLOVENIJE
EVROSISTEM

- Težava
  - Pogled v vse zapise ima samo uporabnik, ki je na vrhu hierarhije
  - Oteženo je odpravljanje napak v aplikaciji
- Rešitev
  - Definiramo posebno intervencijsko vlogo
  - Če ima uporabnik to vlogo, varnostna funkcija vrne pogoj, ki je vedno resničen (1=1).
  - To vlogo lahko začasno dobi informatik po predpisanem organizacijskem postopku

Izjema

BANKA SLOVENIJE
EVROSISTEM

- Namišljena podatkovna baza ne ščiti podatkov pred administratorjem (DBA)

Zaključek

BANKA SLOVENIJE
EVROSISTEM

- Z namišljeno privatno podatkovno bazo izpolnimo varnostne zahteve na enem mestu
- Razvoj uporabniškega vmesnika se poenostavi
- Zahteve so izpolnjene tudi, če uporabnik dostopa do podatkov mimo predvidenega uporabniškega vmesnika
- Težave, na katere smo naleteli, smo uspešno odpravili