# Cap.6. Securitatea bazelor de date

## CUPRINS

1. Concepte generale de securitate

2. Securitatea datelor

3. Politici de securitate

4. Mecanisme de securitate la nivel SGBD





## 1. Concepte generale de securitate

**Arii generale de securitate** a sistemelor informatice:

- securitatea serverelor si a statiilor de lucru;
- securitatea retelei;
- securitatea comunicatiei în retea;
- securitatea aplicatiilor;
- securitatea datelor.

## SECURITATEA SERVERELOR SI A STATIILOR DE LUCRU

**Securizarea serverelor si statiilor de lucru în retea** se realizeaza prin :

- configurarea standard dpdv al setarilor de securitate,
- mentinerea la zi a setarilor de securitate

**Aplicare template-uri de securitate**:

- Active Directory si
- Group Policy (Microsoft Windows)
- Windows Security Essentials.



Curs: BAZE DE DATE ÎN INGINERIE ELECTRICĂ

SECURITATEA SERVERELOR SI A STATIILOR DE LUCRU

## SECURITATEA RETELEI

**Securizarea retelei** este o problema complexa si se realizeaza prin:

- **instalarea si configurarea unui firewall** pentru controlul traficului dinspre/catre Internet,
- **securizarea conexiunilor RAS** (RemoteAccess Service)/**VPN** (Virtual Private Network) pentru utilizatorii mobili sau pentru retele la distanta.





## SECURITATEA COMUNICATIEI ÎN RETEA

**Securizarea comunicatiei in retea** depinde de configuratia retelei.

**Securizare retea cu comunicatie wireless**:

- Criptarea datelor, informaţiile pot fi accesate numai de către utilizatori autorizaţi
- Autentificarea utilizatorilor si a computerelor care încearcă să acceseze reţeaua
- Acces securizat pentru vizitatori (guests)

## SECURITATEA APLICATIILOR

**Securizarea aplicatiilor** presupune

- securizarea aplicatiilor uzuale implementate si
- securizarea aplicatiilor web

## SECURITATEA DATELOR

**Protecţia şi securitatea datelor**: totalitatea mijloacelor, metodelor şi mecanismelor destinate prevenirii distrugerii, modificării sau folosirii neautorizate a informaţiei protejate.

**Concepte de baza** pentru protecţia şi securitatea datelor:

- **Securitatea datelor**: totalitatea măsurilor de protecţie împotriva distrugerii accidentale sau intenţionate, a modificării neautorizate sau a divulgării acestora
- **Caracterul secret**: se aplică la un individ sau organizaţie şi constă în dreptul acestora de a decide ce informaţii se pot folosi în comun şi în ce condiţii
- **Confidenţialitatea datelor**: nivelul de protecţie ce trebuie acordat informaţiei
- **Integritatea**: se referă la restricţia ca sensul datelor să nu difere faţă de cel înscris pe documentul sursă, impunându-se ca datele să nu fie alterate accidental/voit.





## 2. Securitatea datelor

**Nivele de securitate a sistemelor informatice**:

- nivel fizic (hardware),
- nivel sistem de operare şi
- nivel SGBD.

**Securitatea BD multi-utilizatori** permite :

- Controlul accesului la BD
- Acordarea accesului la obiecte specifice din BD
- Confirmarea privilegiilor date si primite

## TIPURI DE SECURITATE

**Securitate BD:**
- securitatea sistemului
- securitatea datelor

**Securitatea sistemului de baze de date:**
- numele utilizatorului si parola,
- spatiul pe disc alocat utilizatorilor, si
- operatiile de sistem permise utilizatorilor

**Securitatea datelor:**
- accesarea si utilizarea obiectelor BD
- actiunile pe care acesti utilizatori le pot efectua asupra obiectelor.





## 3. Politici de securitate

**Politica de securitate:** specifica utilizatorul autorizat si operatiile permise.

**Mecanism de securitate:** permite asigurarea unei anumite politici de securitate.

**Mecanisme de baza la nivelul SGBD**:
- control discretionar al accesului
- control mandatar al accesului

# 4. Mecanisme de securitate la nivel SGBD

## CONTROL DISCRETIONAR AL ACCESULUI

**Control discretionar acces**: bazat pe drepturi de acces = **privilegii pentru obiecte** (tabele si view-uri) si mecanisme pentru a asigna/revoca aceste privilegii utilizatorilor.

**SGBD ofera securizarea operatiilor de administrare a BD** prin:
- ❑ **privilegii pentru creearea, modificarea si stergerea tabelelor** ,
- ❑ **limitarea accesului la anumite BD/ tabele**
- ❑ **specificarea tipului de acces** (Ex: numai citire, acces numai la anumite coloane, acces numai prin intermediul view-urilor sau procedurilor stocate)
- ❑ **creare nivele multiple de securitate**, bazate pe conectarea in sistem





## CONTROL DISCRETIONAR AL ACCESULUI

### Categorii de utilizatori

**Administratorul bazei de date**: **utilizator de nivel înalt** ce are posibilitatea de a acorda accesul utilizatorilor la BD si la obiectele sale.

**Utilizatorii BD:** necesita **privilegii de sistem** pentru a obtine accesul la BD si **privilegii de obiect** pentru a putea manipula continutul obiectelor în BD.

**Utilizatori privilegiati:** li se ofera dreptul de a acorda privilegii aditionale altor utilizatori sau unor **roluri** (grupuri de privilegii adiacente).

## CONTROL DISCRETIONAR AL ACCESULUI

### Instructiuni SQL pentru utilizatori: CREATE USER

```
CREATE USER user_spec[,user_spec]… user_spec:user [IDENTIFIED BY [PASSWORD] 'password' | IDENTIFIED WITH auth_plugin [AS 'auth_string']];
```

Pentru fiecare instructiune CREATE USER se creaza un cont in mysql.user fara privilegii.

Ex.

```
CREATE USER 'student'@'localhost';
CREATE USER 'student'@'localhost' IDENTIFIED BY 'utcn';
```





## CONTROL DISCRETIONAR AL ACCESULUI

### Instructiuni SQL pentru utilizatori: ALTER /DROP USER

```
ALTER USER user_spec[,user_spec]… user_spec:user PASSWORD EXPIRE;
```

Instructiunea ALTER USER modifica userul si duce la expirarea parolei acestui user.

Ex.

```
ALTER USER 'student'@'localhost" PASSWORD EXPIRE;
```

```
DROP USER user[,user]… ;
```

Instructiunea DROP USER sterge userul specificat.

Ex.

```
DROP USER 'student'@'localhost';
```

## CONTROL DISCRETIONAR AL ACCESULUI

### Instructiuni de securitate SQL: GRANT/REVOKE

```
GRANT privilege  [ , privilege… ] ON bd TO user [ , user… ];
```

Unde privilegii pot fi:
- ❑ SELECT: citire coloane
- ❑ INSERT (col-name): inserare valori non null in coloana.
- ❑ DELETE: stergere de valori.
- ❑ REFERENCES (col-name): definire de chei straine (in alte tabele) pentru a referi coloana specificata.

`REVOKE:` revocarea unui privilegiu

`SHOW GRANTS FOR user;` afiseaza privilegiile utilizatorului respectiv





## CONTROL DISCRETIONAR AL ACCESULUI

### Instructiuni de securitate SQL: GRANT/REVOKE

| | |
|---|---|
| **ALL [PRIVILEGES]** | acordă toate privilegiile la un nivel de acces specificat cu excepţia GRANT OPTION |
| **ALTER** | permite folosirea clauzei ALTER TABLE |
| **CREATE** | permite crearea de baze de date şi tabele |
| **CREATE VIEW** | permite crearea şi modificarea vederilor |
| **DELETE** | permite folosirea clauzei DELETE |
| **DROP** | permite ştergerea bazelor de date, vederilor şi tabelelor |
| **GRANT OPTION** | permite ştergerea sau adăugarea de privilegii unui cont |
| **INDEX** | permite crearea şi modificarea indecşilor |
| **LOCK TABLES** | permite folosirea LOCK TABLES pentru tabele unde sunt privilegii SELECT |
| **SELECT** | permite folosirea clauzei SELECT |
| **SHOW DATABASES** | permite folosirea SHOW DATABASES |
| **SHOW VIEW** | permite folosirea SHOW CREATE VIEW |
| **TRIGGER** | permite operaţiile cu triggere |
| **UPDATE** | permite folosirea clauzei UPDATE |
| **USAGE** | este sinonim cu “no privileges” |

## CONTROL DISCRETIONAR AL ACCESULUI

### Instructiuni de securitate SQL: GRANT/REVOKE

**Exemplu MySQL:**

```
CREATE USER 'student'@'localhost' IDENTIFIED BY 'mypass';

GRANT ALL ON db1.* TO 'student'@'localhost';
GRANT SELECT ON db2.catalog TO 'student'@'localhost';
GRANT SELECT, INSERT ON *.* TO 'student'@'localhost';

REVOKE INSERT ON *.* FROM 'student'@'localhost';
```





## CONTROL DISCRETIONAR AL ACCESULUI

### Instructiuni de securitate SQL: GRANT/REVOKE

**Exemplu MySQL: acordare privilegii globale**

```
GRANT ALL ON *.* TO 'someuser'@'somehost';
GRANT SELECT, INSERT ON *.* TO 'someuser'@'somehost';
```

**Exemplu MySQL: acordare privilegii asupra bazei de date**

```
GRANT ALL ON mydb.* TO 'someuser'@'somehost';
GRANT SELECT, INSERT ON mydb.* TO 'someuser'@'somehost';
```

**Exemplu MySQL: acordare privilegii asupra tabelelor bazei de date**

```
GRANT ALL ON mydb.mytbl TO 'someuser'@'somehost';
GRANT SELECT, INSERT ON mydb.mytbl TO 'someuser'@'somehost';
```

## CONTROL DISCRETIONAR AL ACCESULUI

### Instructiuni de securitate SQL: GRANT/REVOKE

**Exemplu MySQL: acordare privilegii de coloane**

```
GRANT SELECT (col1),INSERT(col1,col2)ON mydb.mytbl TO
'someuser'@'somehost';
```

**Exemplu MySQL: acordare /retragere privilegii asupra utilizatorilor**

```
GRANT ALL ON test.* TO 'student'@'localhost' …
REVOKE ALL PRIVILEGES, GRANT OPTION FROM 'student'@'localhost';
//retragerea tuturor privilegiilor utilizatorului
```





## CONTROL DISCRETIONAR AL ACCESULUI

### Securitate prin view-uri

- view-urile pot fi utilizate pentru prezentarea anumitor informatii ascunzand campurile protejate din tabele
- alaturi de comenzile *GRANT*/*REVOKE*, view-urile constituie instrumente puternice de control al accesului
- se pot specifica privilegii de acces la nivel de camp

## CONTROL MANDATAR AL ACCESULUI

**Control mandatar al accesului**: bazat pe politici de nivel sistem si **clase de securitate** ce nu pot fi modificate de utilizatori individuali:

- ❑ fiecarui obiect din BD i se asigneaza o clasa de securitate.
- ❑ fiecarui subiect (user / program) i se asigneaza o caracteristica de acces aferenta unei clase de securitate.
- ❑ reguli bazate pe clasele de securitate guverneaza "cine va putea citi/scrie?" "care obiecte?" din BD.

NU toate SGBD comerciale suporta acest tip de securizare.





## Test

**Care instructiune SQL, ofera toate drepturile de administrare userului "admin" asupra tabelului "Angajati" din baza de date "db"**

a) GRANT ALL FROM db.Angajati ON TO admin ;

b) GRANT ALL TO admin WHERE FROM db.Angajati;

c) GRANT ALL WHERE FROM Angajati .db TO admin;

d) GRANT ALL ON db.Angajati TO admin;

## Test

**Care instructiune SQL, ofera toate drepturile de administrare userului "admin" asupra tuturor tabelelor din baza de date "db"**

a) GRANT ALL ON *.* TO admin ;
b) GRANT ALL ON db.* TO admin;
c) GRANT ALL TO admin FROM db.*;
d) GRANT ALL WHERE FROM Angajati .* TO admin;





## Test

**Care instructiune SQL, ofera drepturile de citire a coloanei pret si inserare de valori in coloana cod pentru userul "admin" in tabela "produse " din baza de date "db"?**

a) GRANT SELECT (pret), INSERT (cod) ON db.produse TO admin;
b) GRANT SELECT , INSERT ON db.PRODUSE TO admin;
c) GRANT ALL TO dv.* FROM admin;
d) GRANT SELECT (pret),INSERT(cod) TO admin ON db.produse;

## Ora viitoare

Criptarea datelor

Bazele de date publice – motoare de cautare

Tehnici de căutare şi regăsire a informatiei în Internet - motoare de căutare