

ADMINISTRAREA BAZELOR DE DATE

CURS 11. SECURITATEA DATELOR (PARTEA A 2-A)

Conf. Dr. Ing. Delia-Alexandrina Mitrea
Delia.Mitrea@cs.utcluj.ro

Cuprins:

- Acordarea si revocarea autoritatii
- Tipuri de privilegii
- Roluri si grupuri de autorizare
- Alte mecanisme - pt. asigurarea securitatii BD
 - Vederi
 - Proceduri stocate
 - Securitate la nivel logic
- Auditarea bazei de date
- Securitate externa
- Planificarea job-urilor si securitatea BD
- Securitate non-SGBD

➤ **Acordarea si revocarea autoritatii**

- **ABD** – controleaza securitatea BD si autorizarea utilizand **Limbajul de Control al Datelor (LCD)**
- **Instructiunile LCD** – controleaza accesul utilizatorilor asupra obiectelor si comenzilor din BD
- **2 tipuri de instructiuni LCD:**
 - **GRANT** – asigneaza permisiuni unui anumit utilizator al BD
 - **REVOKE** – anuleaza aceste permisiuni
- **GRANT** => 2 liste de parametri:
 - 1 lista de privilegii pt. utilizatori
 - 1 lista de utilizatori carora li se acorda privilegii
- Pt. a invoca instructiunile de tip GRANT -> utilizatorul trebuie sa fie proprietarul obiectului invocat din BD, sa aiba autoritate de grup de nivel inalt, sau sa fi primit privilegiile initiale in combinatie cu optiunea **WITH GRANT OPTION**

- **WITH GRANT OPTION** – permite transferul autoritatii pt. a facilita acordarea privilegiilor in grupuri cat mai extinse
- Utilizarea acestei clauze – depinde de tipul de instalare ⇔ dc. practica sau nu *administrarea centralizata sau **descentralizata** a privilegiilor*
 - **Administrare descentralizata** - usor de stabilit, mai dificil de controlat
 - **Administrare centralizata** - usor de stabilit, dar – presiune crescuta asupra unui singur ABD ⇔ singurul arbitru al privilegiilor
- A se evita utilizarea instructiunilor **GRANT** si **REVOKE** dintr-un program aplicatie -> acestea trebuie executate de utilizatori – privilegii corespunzatoare

➤ Tipuri de privilegii

- Diferite tipuri de privilegii – pot fi acordate sau revocate utilizatorilor BD
- SGBD – privilegii de baza – abilitatea de a accesa datele de a crea obiectele BD, de a apela functii sistem
+ privilegii aditionale
- Privilegii comune - SGBD-uri moderne:
 - Privilegii **la nivel de tabel** - accesare & modificare date din tabele
 - Privilegii **la niv. obiectelor BD** - controleaza cine poate crea obiecte noi sau sterge obiectele existente
 - Privilegii **la nivel de sistem** - extinse la nivelul S.O.

- Privilegii **la nivel de program** – cine poate crea, modifica si utiliza programele BD
 - Privilegii **la niv. procedurilor stocate** – cine poate executa proceduri stocate & functii specifice
-
- **Acordarea privilegiilor la nivel de tabel**
 - Permit utilizatorilor sa acceseze tabele, vederi si coloane in tabele si vederi
 - Privilegii pt. tabele si vederi:
 - SELECT - vizualizarea datelor din tabele/vederi
 - INSERT - inserarea inregistrarilor in tabele/vederi
 - UPDATE – modificarea tabelor/vederilor
 - DELETE – stergerea inregistrarilor din tabele/vederi
 - ALL – Select, Insert, Update, Delete din tabele/vederi

▪ **Exemple – Microsoft SQL Server:**

```
GRANT DELETE on Titles to user7;
```

- Acordarea privilegiului de stergere a datelor din tabelul *Titles*, pt. *user7* – ***la nivel de tabel***

```
GRANT UPDATE on Titles (au_id) to user7;
```

- Acordarea privilegiului de modificare a datelor din coloana *au_id*, din tabelul *Titles*, pt. *user7* – ***la nivel de coloana***

■ Acordarea privilegiilor asupra obiectelor BD

- Controleaza ce utilizatori au drepturi/privilegii sa creeze structuri in BD
- SGBD => optiuni de creare a privilegiilor pe fiecare tip de obiect - ex. baze de date, spatii tabelare (tablespaces), tabele, indecsi, triggeri si tipuri de date def. de utilizatori

```
GRANT CREATE table,  
CREATE index  
TO user5,  
user9;
```

- Acordarea permisiunii de a crea tabele si indecsi utilizatorilor *user5* si *user9*

- Abilitatea de a crea obiecte BD – rezervata ABD
- Dc aceste privilegii – acordate altora – nr. obiectelor BD => dificil de controlat



- ABD – sa pastreze aceste privilegii pt. sine – cu mici exceptii – ex. Administratorii de Sistem sau dezvoltatori f. experimentati (priceputi)

▪ Acordarea privilegiilor la nivel de sistem

- Controleaza utilizarea facilitatilor SGBD si executarea comenzilor SGBD de catre utilizatori
- Ex. de privilegii sistem: arhivarea log-urilor BD, oprirea/pornirea serverului BD, monitorizarea performantelor, gestiunea depozitarii datelor, gestiunea cache-ului BD
- Nu pot fi acordate la nivelul BD; sunt adesea rezervate ABD sau Admin de Sistem
- Ex.: **GRANT TRACE
TO user6;**
 - Acorda utilizatorului *user6* permisiunea de a incepe *urmarirea sistemului* in vederea *monitorizarii performantelor* acestuia

- **Acordarea privilegiilor la nivel de program si de proceduri stocate**

- Acordarea privilegiilor de tip EXECUTE => acorda utilizatorilor permisiunea de a executa un program sau o procedura stocata
- Ex.:

```
GRANT EXECUTE on proc1  
TO user1, user9;
```

Acorda utilizatorilor *user1* si *user9* permisiunea de a executa procedura *proc1*

- Aceste privilegii – mai usor de controlat decat acordarea de privilegii pe coloane si tabele individuale

▪ Acordarea de privilegii “user-ului” PUBLIC

- In loc sa acorde privilegii unui anumit utilizator - ABD poate alege sa acorde privilegii “user-ului” PUBLIC => SGBD va acorda acele privilegii oricui se va loga in sistem
- Grant-urile catre PUBLIC – nu vor putea fi acordate prin intermediul optiunii WITH GRANT OPTION
- **Ex.:**

GRANT DELETE on titles to PUBLIC;

- Se acorda tuturor utilizatorilor privilegiul de a sterge inregistrari din tabelul titles

▪ **Revocarea privilegiilor**

- Instructiunea **REVOKE** – anulara (revocarea) privilegiilor acordate anterior
- Privilegiile ramase – vor fi anulate de catre sistem in momentul stergerii de catre SGBD a obiectelor
- Ex.:

```
REVOKE UPDATE on titles (au_id)  
from user7;
```

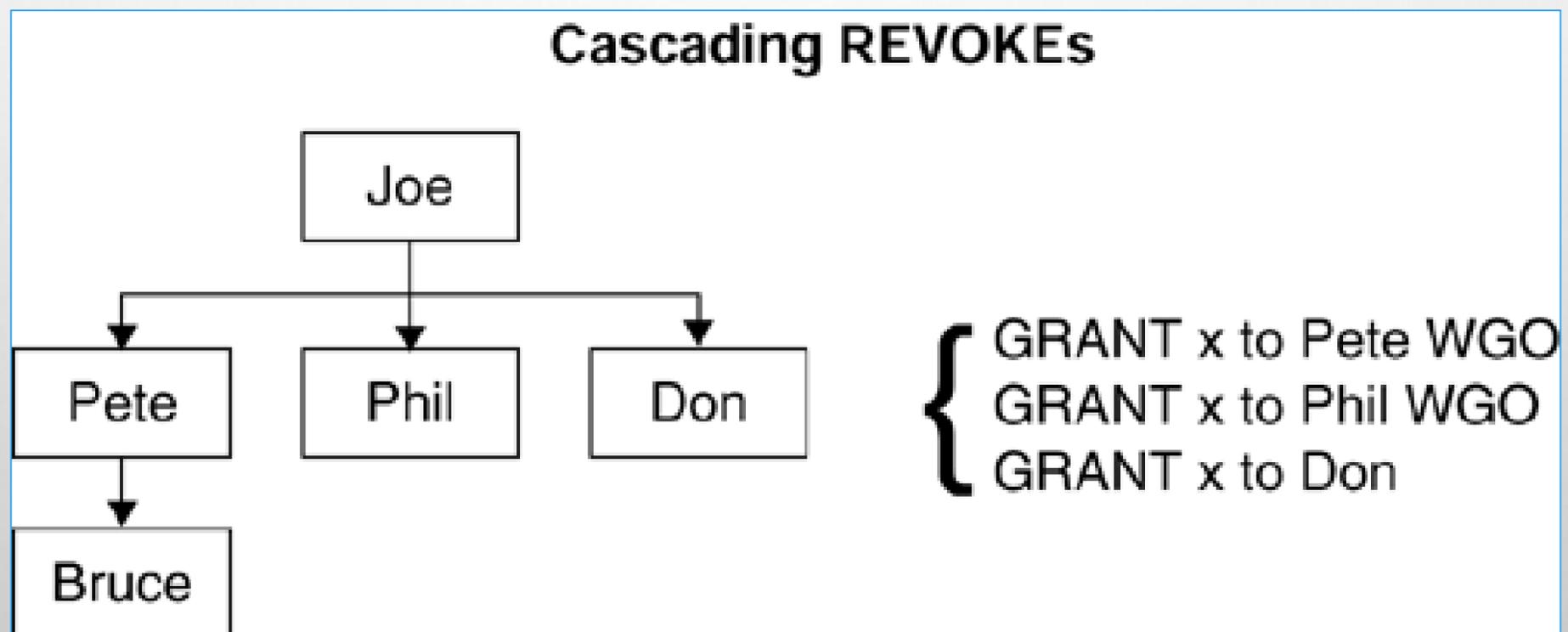
=> Revocarea dreptului de actualizare (update) a campului *au_id* din tabelul *titles*, utilizatorului *user7*

- Anulara unui privilegiu de tip PUBLIC => nu va anula acel privilegiu pt. acei utilizatori carora li s-a acordat acest drept printr-o instructiune GRANT separata

■ Cascadarea revocarilor

- Atunci cand anumite privilegii sunt revocate => SGBD decide daca sunt necesare si alte revocari => **cascadarea revocarilor**

- **Ex.: ierarhie de autoritate**



(1) JOE – acorda dreptul X lui Pete si lui Phil utilizand optiunea WITH GRANT OPTION; acorda dreptul X lui Don fara aceasta optiune

(2) Revocarea privilegiului X pt. utilizatorul JOE => JOE nu va mai avea privilegiul X, iar SGBD va revoca de asemenea acest drept lui Pete, Phil si Don

- Pt. ca i s-a revocat privilegiul lui Phil => aceasta revocare se va cascada si catre Bruce

- Pt. a minimiza impactul cascadarii revocarilor => a se evita acordarea privilegiilor folosind optiunea WITH GRANT OPTION => usurinta in gestionare si administrare a unei infrastructuri de securitate viabile a SGBD

▪ Cronologie si revocari

- Succesiunea in timp a instructiunilor GRANT si REVOKE – de o importanta deosebita
- Ex:



```
GRANT DELETE on titles to public;  
COMMIT;  
REVOKE DELETE on titles from userx;
```

- Se acorda permisiunea DELETE tuturor utilizatorilor
 - Se retrage dreptul de stergere utilizatorului *userx*
-
- Anumite SGBD-uri – ex.: DB2 => nu vor permite asemenea excluderi – autoritatea PUBLIC suprascrie orice revocari
 - Alte SGBD-uri – ex. Microsoft SQL Server – permit asemenea operatii

▪ **Raportarea problemelor de securitate**

- ABD – monitorizarea si raportarea privilegiilor detinute de utilizatori
- Securitatea BD – mentinuta in Catalogul Sistem
- ABD – poate folosi SQL pt. a regasi informatia dorita din tabelele catalogului sistem
- Anumite SGBD-uri – furnizeaza vederi si proceduri stocate sistem care simplifica regasirea informatiilor de Securitate
⇒ ABD – trebuie sa asigure securitatea Catalogului Sistem

- Cerintele de securitate si asteptarile utilizatorilor – evolueaza in timp
 - Odata cu dezvoltarea de noi aplicatii & modificarea cerintelor de business => securitatea BD va necesita modificari
 - *Review-urile de securitate* - trebuie realizate in mod regulat => securitatea BD va continua sa corespunda cerintelor actuale ale utilizatorilor

➤ Roluri si grupuri de autorizare

- In afara de a acorda privilegii utilizatorilor individuali, SGBD – mai furnizeaza capabilitatea de a asigna:
 - Privilegii specifice unui anumit rol
 - Grupuri de privilegii pt. utilizatori
- **Roluri**
 - **Un rol** – utilizat pentru a acorda (conferi) unul sau mai multe privilegii pre-asignate unui utilizator
 - **Un rol** ⇔ **o colectie de privilegii**
 - ABD – poate crea un rol si sa asigneze anumite privilegii acelui rol; apoi, rolul poate fi asignat unuia sau mai multor utilizatori => simplificarea administrarii securitatii BD

|

```
CREATE role MANAGER;  
COMMIT;  
GRANT select, insert, update, delete on employee to  
MANAGER;  
GRANT select, insert, update, delete on job_title to  
MANAGER;  
GRANT execute on payroll to MANAGER;  
COMMIT;  
GRANT MANAGER to user1;
```



ABD poate crea un rol si asigna privilegii aceluia rol

- **Grupuri**

- Autoritatea la nivel de grup – similara cu rolurile
- Fiecare SGBD => grupuri predefinite care nu pot fi modificate
- SGBD – implementeaza securitatea la nivel de grup in moduri diferite si cu diferite nume de grup, resp. privilegii
- Similaritati intre SGBD – uri – grupuri predefinite:
 - **System Administrator (SYSADM, SA)** – cel mai puternic grup din SGBD
 - => utilizatorul poate sa execute toate comenzile BD si sa acceseze toate BD si obiectele;
 - => responsabil de instalarea SGBD-ului;
 - => proprietarul resurselor sistem si al catalogului sistem

- **Database Administrator (DBADM, DBA)**

- ⇒ Privilegii asupra unei baze de date specifice

- ⇒ Abilitatea de a accesa, fara a modifica tabelele de date

- ⇒ Stergerea si modificarea oricaror obiecte din BD: spatii tabelare, tabele, indecsi

- **Database Maintenance (DBMAINT)**

- ⇒ Privilegii specifice pt. mentenanta obiectelor BD – e.g. abilitatea de a rula utilitare specifice; de a lansa comenzi specifice;

- ⇒ Acordat pt. o anumita BD

- **Security Administrator (SSO)**

- ⇒ Acordarea sau revocarea (Grant/Revoke) privilegiilor de securitate într-un SGBD

- ⇒ orice activitate referitoare la securitatea BD, inclusiv administrarea numelor de utilizator (loginuri) și parole, auditare, configurarea securității

- **Operations Control (OPER sau SYSOPR)**

- ⇒ Task-uri operationale la nivelul BD (ex. backup și restore)

- ⇒ Terminarea forțată a unor task-uri aflate în execuție

- **Limitarea numărului de utilizatori cu rolul SA/SYSADM**

- O singură organizație – ar trebui să limiteze numărul de utilizatori cu rolul SA sau cu autoritate la nivel de grup
 - Doar la nivel de corporație – ABD sau programatorii de sistem -> să primească acest nivel de autoritate

➤ Alte mecanisme - pt. asigurarea securitatii BD

• Utilizarea vederilor

- Cea mai mare parte a functiilor de securitate – asigurate prin functiile native ale SGBD
 - Simplificarea anumitor aspecte ref. la securitate => crearea vederilor pt. protejarea datelor
 - **Ex.**
 - BD organizationala – contine o tabela Angajati – date despre angajati – Nume, Prenume, Adresa, Telefon, Salar
 - Grant SELECT pe angajati => angajatii – salariile altor angajati!
- => crearea unei vederi pt. rafinarea vizualizarii

```
CREATE view emp_all
AS
SELECT first_name, last_name,
middle_initial, street_address, state,
zip_code
FROM employee;
```



- Omiterea informatiilor senzitive legate de salar si telefon ⇔
“restrictie verticala” – clauza SELECT
- Specificarea securitatii la nivel de coloana – necesara organizatiei

- Securitate la nivel de linie ⇔ “row level security” – restricție orizontală - prin intermediul clauzei WHERE

```
CREATE view emp_dept20
AS
SELECT first_name, last_name,
middle_initial,
street_address, state, zip_code
FROM employee
WHERE deptno = 20;
```

- Dc. se specifica WITH CHECK OPTION => verificările se vor face și la INSERT, UPDATE, DELETE

- **Utilizarea procedurilor stocate pt. securitate**

- Procedurile stocate => un nivel aditional de securitate
- Privilegiul (dreptul) de a executa o procedura stocata – acordat (granted) sau revocat (revoked) in mod explicit – indep. de securitatea implem. in tabele
- Proc. stocate => accesarea subseturilor de date la nivel de linie sau de coloana
- Dreptul de a executa aceste proceduri stocate – conferit in mod adecvat utilizatorilor => utiliz. – op. pe tabele chiar daca nu au privilegii asupra acestora
- Proc stocate => imbunatatirea performantelor - dc. algoritmi sau procedurile – codificate corespunzator

- **Securitate la nivel logic**

- Uneori – necesara implementarea securitatii prin intermediul unor algoritmi specifici
- Ex. – un grup de utilizatori trebuie sa acceseze un anumit tabel doar intr-o anumita perioada din zi => codificarea prin intermediul unei proceduri stocate
- Anumite SGBD-uri => functii specifice pt. implementarea securitatii
 - Ex. **Oracle Virtual Private Database** – faciliteaza controlul accesului la nivel de linie (rand) ⇔ asocierea uneia sau mai multor politici de securitate cu tabelele sau vederile din BD - bazate pe *predicate SQL* -> *actioneaza prin intermediul clauzei WHERE*
 - ⇔ crearea unor vederi dinamice

➤ **Auditarea BD**

- ↔ O facilitatea a SGBD – permite ABD sa urmareasca exploatarea resurselor si privilegiilor BD
- Atunci cand auditarea este permisa (“enabled”) => SGBD va produce o “pista” de audit a operatiunilor BD – ce obiect a fost impactat, cine a realizat operatiile, cand anume
 - Dep. de nivelul de audit suportat de SGBD – inregistrarea unui raport al datelor care au fost modificate si de catre cine
 - => *important datorita amenintarilor existente (Threats to Security)*

○ **Tipuri de amenintari (Threats to Security)**

- Agentii externi care pot accesa datele companiei
=> pot compromite si securitatea datelor
- Studii => 60% - 80% dintre amenintari – interne –
in cadrul organizatiei
 - Ex. tipic – un angajat nemultumit sau fost
angajat al companiei – access validat la
SGBD
- Auditarea – cruciala – determinarea - unui acces
neautorizat la BD - de catre un utilizator
neautorizat

- **Procesul de auditare** - urmareste toate actiunile unui anumit utilizator - odata ce acesta a primit access la BD
 - Are loc - **dupa realizarea activitatilor (post-activity)**
 - **Nu implica luarea unor masuri prohibitive** asupra accesului la BD
 - **Ajuta la promovarea integritatii datelor** – detectarea breselor de securitate ⇔ detectia intruziunilor
 - **Un sistem auditat** – descurajant – modificarea frauduloasa a datelor de catre utilizatori – ajuta la identificarea “infiltrarilor”
 - **O pista de audit** – utila in situatii multiple – practicile de business & politicile de securitate ale companiei => modul de urmarire a operatiilor/modificarilor facute asupra datelor de catre utilizatori; rapoarte cerute de catre autoritati (ex. guvernamentale)

- **Facilitate tipica de audit** => auditarea la diferite niveluri in cadrul SGBD :
 - nivelul BD
 - nivelul obiectelor din BD
 - nivelul utilizatorului

- **Una dintre cele mai mari probleme** => *degradarea performantelor SGBD*
 - **Pistele de audit** ⇔ suficient de detaliate – capturarea imaginilor dinaintea modificarii/dupa modificare (before/after) => degradarea performantelor SGBD per ansamblu
 - + **datele de audit** – stocate pe disc => probleme <- nr mare de modificari
 - => *majoritatea sistemelor de audit* – permit crearea selectiva a record-urilor specifice => minimizarea problemelor de performanta & stocare

▪ **Puncte comune – auditare – SGBD-uri:**

- Monitorizarea actiunilor/tentativelor de login/logoff
 - Urmarirea actiunilor de restartare a serverelor de BD
 - Urmarirea comenzilor realiz. de utilizatori - privilegii de SYSADM
 - Tentative de violare a integritatii datelor ↔ incalcarea constrangerilor de integritate
 - Urmarirea op. de SELECT, INSERT, UPDATE, DELETE
 - Executia procedurilor stocate
 - Tentative nereusite de a accesa o BD sau un tabel – esecuri de autorizare
 - Modificari asupra tabellelor sistem
 - Operatii asupra inregistrarilor (la nivel de rand)
-
- Pot fi achizitionate instrumente aditionale => analiza a log-urilor de tranzactii + rapoarte formatate & instrumente grafice de raportare – ex. Tableau <https://www.tableau.com/>

▪ **Auditare BD pe Internet (web-site-uri)**

- Web-site-uri – auditarea BD \Rightarrow mare consumatoare de resurse - probleme la umplerea cozii cu date pt. audit (task-urile generatoare de date – asteapta resetarea procesului de audit) \Rightarrow luarea in considerare a unei cozi de dim. mai mari; incetarea auditarii – dc. performantele se degradeaza considerabil
- Plasarea tabelor catalogului sistem care stocheaza info legate de Securitate – disc separat, inactiv
- Asigurarea – tablele utilizate pt. a stoca date legate de audit – nu se umplu excesiv (\Rightarrow dezactivarea procesului de audit, pierderea inregistrarilor & anulara task-urilor de audit care trimit date in aceste table)

➤ **Securitate externa**

- ABD – trebuie sa se asigure ca anumite resurse ale SGBD – protejate de accesul extern (din afara SGBD)
- Dc. resursele BD nu sunt accesate utilizand comenzi ale SGBD sau instruct. SQL => mecanismele de securitate nu se pot baza pe procesul de autentificare
- ABD – sa se focalizeze pe seturile de date si fisierele utilizate de catre SGBD:
 - Fisiere de date din Catalogul Sistem
 - Fisiere log active/arhivate
 - Seturi de date utilizator sau spatii tabelare
 - Seturi de date pentru indecsi
 - Fisiere de date de audit
 - Fisiere de urmarire a performantei
 - Programe si fisiere cu script-uri (cod sursa & executabil)

- Utilizatorii “ingeniosi” – ar putea detecta formatul acestor fișiere & accesa în mod neautorizat datele – neprotejate corespunzător
- Un nivel adițional de protecție \leq **compresia datelor din SGBD** \Rightarrow complicarea operațiunii de intruziune a hackerilor
- **Incriptarea datelor** – software specific \Rightarrow codificarea datelor lizibile într-un format specific – fișierele devin nelizibile în absența cheii de criptare
- Securitate adițională pt. resursele SGBD - ref la stocarea fizică și spațiul de adresare utilizat, consola, fis. de instalare a SGBD

➤ Planificarea job-urilor & securitatea SGBD

- Asignarea autoritatii planificatorului de job-uri
 - ABD – deterimna modalitatea optima – at. cand se utilizeaza soft-uri aditionale – ex. CA-7, Control-M, AutoSys
- A nu se asigna aceasta autoritate rolului SYSADM
=> job-urile – orice task/operatii in BD
- ABD – sa determine cum se poate acorda autoritate pt job-uri specifice
- *Eroare comuna de securitate* – integrarea - parole actuale - in cadrul job-urilor si script-urilor

➤ **Securitate non-SGBD**

- ABD – autoritate (niv. inalt) si asupra Sistemului de Operare (S.O.) – pt. a putea realiza administrarea si gestionarea datelor din BD organizationala
- Ex. – in UNIX – anumite task-uri de instalare – autoritate de tip *root*
- 2 modalitati:
 - Conferirea autoritatii de tip *root* - ABD
 - Asignarea task-ului catre administratorul de sistem (SA)
- ABD & SA - cooperare stransa

➤ Concluzii

- Securitatea BD – o coordonata f. importanta – privind atributiile ABD
- Fara un plan bun de securitate => integritatea organizatiei va fi compromisa
- ABD – sa foloseasca mecanismele de securitate pe care le are la dispozitie => doar utilizatorii autorizati sa acceseze & modifice date din BD organizationala
- ABD – sa implementeze operatii de audit – verificarea mecanismelor de securitate implementate in SGBD

Bibliografie

[1] Craig S. Mullins, “Database administration. The complete guide to practices and procedures. Ch. 14. Database Security”, Addison Wesley, 2012

Mulumesc pentru atentie!