METODE DE SECURIZARE A UNEI BAZE DE DATE

COSTIUC Irina

Universitatea Tehnică a Moldovei

Abstract: *În acest articol sînt analizate cele mai optimale metode şi tehnici pentru crearea sistemului complex de securizare a unei baze de date, acestea fiind grupate după anumite criterii şi relatate într-o formă detaliată. De asemenea, sînt scoase în evidenţă avantajele şi dezavantajele fiecărei metode.*

Cuvinte cheie: *bază de date, utilizatori, securizare, confidenţialitate.*

1. Introducere

Cunoastem bine faptul că activităţile diferitor organizaţii din lume (corporaţii, înreprinderi mari, mici, de stat), depind tot mai mult de tehnologiile informaţionale, astfel putem deduce că problema protecţiei bazelor de date devine tot mai actuală. Pericolul de pierdere a informaţiei confidenţiale a devenit ceva obişnuit, însă şi un lucru riscant pentru activitatea unei organizaţii. Fiecare esec în procesarea bazelor de date poate paraliza activitatea unor corporaţii întregi, bănci, servicii internet, ceea ce poate duce la pierderi financiare colosale. Deci, protecţia datelor este o sarcină ce trebuie pus pe primul plan la crearea unei baze de date.

Astfel, pentru a asigura securitatea unei baze de date, este necesar de realizat anumite etape, ce vor contribui la evitarea spargerii bazei de date: stabilirea dreptului de access la elementele bazei de date, introducerea parolei specifice, criptarea datelor si programelor.

2. Stabilirea dreptului de access la Baza de Date si elementele ei

La cel mai elementar nivel, conceptul de securitate a bazei de date este unul simplist, aici este necesar de păstrat doua principii fundamentale: controlarea autorizărilor si autentificărilor. Prin controlarea autorizărilor se subînţelege nivelul de acces la date în dependenţă de tipul autentificării. Controlul autorizătrior este bazat pe faptul ca fiecărui utilizator sau proces îi este încredinţat un anumit set de acţiuni, pe care aceasta le poate efectua, în interacţiune cu anumite elemente din Baza de Date. Iar prin autentificare, se confirmă faptul ca utilizatorul sau procesul este obiectul căruia i se permite de a efectuia o activitate.

Sistemul de autorizare se formează dintr-o structură ierarhică. Cel mai înalt nivel a acestei structuri îl ocupă administratorul bazei de date. În mod tradiţional, numai administratorul are dreptul de a crea utilizatori noi si de a atribui anumite permisiuni la accesarea Bazei de Date. Structura ierarhică sistemului de autorizare al unei BD poate fi creată în dependenţa de scopul pe care îl urmăreşte aceasta şi nivelul accesibilităţii la ea, cele mai des utilizate fiind:

- Diferite tipuri de utilizatori pot avea access diferit la unul si acelaşi obiect, spre exemplu: Numai Citireea Datelor; Redactarea şi Cititrea; Copierea elementelor etc. Aceasta se realizează prin crearea în BD, a unui nou tip de obiect – utilizatorii. Astfel, fiecărui utilizator al bazei de date i se atribuit un ID specific si o parola unică. Adriministratorului îi este cunoscut numai ID-ul utilizatorului, iar parola este un atribut secret, cunoscut doar de utilizator.
- Un alt tip de access la date se determină prin gruparea utilizatorilor în clase. În mod standart, regăsim grupul Public, căruia îi sint oferite minimum instrumente şi acces la BD. Fiecare utilizator nou creat este automat introdus în acest grup. Privilegiile si accesul la BD sint specifice fiecarui grup, în care utilizatorii pot fi încadraţi doar de administrator.
- În ultimile versiuni ale produselor SBGD a aparut un nou atribut numit ”rol”- permisiuni determinate aparte. Este posibilă crearea rolurilor noi, şi specificarea tipului specific de access. Aceasta a optimizat controlul asupra privilegiilor pentru utilizatori. Deasemenea, utilizatorilor le este oferită posibiliatea de a fi încadraţi în unul sau mai multe roluri.

3. Protejarea BD prin parole

Parola este destinată pentru a proteja BD untr-un mod simplu si eficient contra accesului neautorizat. Parola este un atribut stabilit de către utilizator şi cunoscut doar de acesta. Administratorul are access redus la parolă, ba chiar mai mult - nu are posibilitatea de a o afla. Înregistrarea si stocarea parolelor se efectuează de către SGBD, ele fiind păstrate în fişierele de sistem ale BD. Deci, este dificil de a găsi şi a determina parola, chiar aproape imposibil. Astfel, pentru a indentifica utilizatorului şi tipul de access al acestuia, este de ajuns introducerea ID-ului utilizatorului şi a parolei de access, care se transmite în mod criptat.

4. Criptarea Datelor

Criptarea datelor se utilizează pentru a evita citirea informației de către alte softuri neautorizate, de asemenea criptarea textelor sursă permite ascunderea conţinutului de la utilizatorii neînregistraţi. În baze de date cu conținut confidențial utilizarea metodelor criptografice reprezintă un punct important.

Există diverse metode de criptare a informației, atît cu utilizarea unei singure chei (cheie simetrică), cît si utilizarea cheilor individuale a fiecărui utilizator (cheie asimetrică).

Criptarea cu o cheie simetrică este determinată prin procesul de criptare şi decriptare cu o cheie secretă. Avantajul acestei metode de criptare constă în procesarea optimală a criptării. Dezavantajul este că odată cu determinarea cheiei secrete există un risc sporit de scurgere de informatii.

Criptarea cu o cheie asimetrică este determinată prin utilizarea unei chei publice pentru decriptarea anumitor documente cu importanță mică, și a unei chei confidețiale, care permite decriptarea întreg continutului, inclusiv și a elementelor confidențiale. Cheia secretă este cunoscută de un număr minim de persoane. Criptarea prin utilizarea ultimei metode este mult mai sigură, avînd avantaje mai multe, inclusiv în domeniul securității. Iar dezavantajul ar fi necesarul de investiții mai mari în dizevoltarea criptării.

Implementarea acestor metode de criptare se efectuează prin două moduri. Cel mai simplu consta din procedura de apel la un anumit fișier din BD, ca apoi să fie exportat și decriptat pe un suport extern dependent de BD, și invers. Avantajul constă în procesarea mai optimală a criptării, în același timp, un eșec în sistem poate afecta procesul criptografic astfel, încît BD criptată va rămîne indisponibilă pînă cînd nu se va implementa procesul de analiză criptologică, care durează timp.

Al doilea mod implică îndeplinirea apelurilor de la SGBD fară decriptarea informației. Căutarea fișierelor, înregistrărilor, grupurilor de oameni nu necesită decriptarea fiecărui element print export pe memorie externă. Aceasta se face în BD direct. Astfel de regim este posibil, dacă procedura de criptare este înclusă în SGBD. Realizarea acestui mod de criptare depinde de complexitatea SGBD-ului. De regulă, astfel de mod de operare se formează încă la nivelul realizarii SGBD. Iar ca avantaj, acest mod oferă nivel înalt de securitate.

5. Concluzii

Analizînd elementele necesare pentru securizarea unei BD, s-au arătat metodele optime pentru construirea accesului securizat la aceasta. Deasmenea, au fost accentuate nivelele de access la baza de date, structura lor și posibilitățile oferite de acestea. În dependență de scopul unei BD se determină tipul structurii ierarhice și necesarul utilizării unei parole pentru evitarea accesului neautorizat. Iar în depdendență de conținutul confidențial al BD, au fost menţionate metode și tehnici criptologice pentru evitarea scurgerii contentului important. Astfel, reieșind din importanța securizării BD, această temă trebuie să fie obiectul unei cercetări continuie pentru implementarea cu succes în practică.

Bibliografie

1. Особенности защиты информации в базах данных. [Resursă electronică]. – Regim de Access: http://sumk.ulstu.ru/docs/mszki/Zavgorodnii/11.7.html
2. Защита информации в базах данных. [Resursă electronică]. – Regim de Access: http://www.intuit.ru/studies/courses/1001/297/lecture/7423
3. Защита Баз Данных. [Resursă electronică]. – Regim de Access: http://www.bseu.by/it/tohod/lekcii9_2.htm
4. Безопасность баз данных [Resursă electronică]. -Regim de acces: http://www.rus-lib.ru/book/28/ps/05/396-422.html