Sergiu PADURE, ASEM

SECURITATEA BAZELOR DE DATE CORPORATIVE

Bazele de date constituie unul din componentele cele mai importante a oricărui sistem informatic mare, care păstrează şi prelucrează diverse date, informaţii. Acestea pot fi sisteme de gestiune a documentelor şi a evidenţei contabile, sisteme de billing şi de management al conţinutului (CMS), sisteme de gestiune a proceselor tehnologice la producere etc. Deoarece bazele de date conţin toată informaţia valoroasă despre companie, clienţii săi, activitatea financiară, ele reprezintă unul din factorii critici în structura organizaţiei, fapt care determină cerinţe sporite de confidenţialitate, integritate şi acces la date.

Riscurile care pot interveni în acest context pot apărea atât din mediul extern (viruşi, hackeri, concurenţi etc.), cât şi interni (furtul, acţiuni ale lucrătorilor necinstiţi, erori şi scăpări din vedere ale personalului de deservire şi a utilizatorilor ş.a.). De asemenea, e necesar de luat în consideraţie şi fiabilitatea sistemelor, a SGBD-urilor, mijloacelor tehnice care se pot supune unor factori, cum ar fi: incendiile, calamităţile naturale etc. ***Astfel, pentru a găsi soluţii, iniţial e necesară stabilirea punctelor precare în bazele de date:***

1. *Limbajul SQL – un instrument puternic de interogare a datelor*, însă de asemenea permite răufăcătorilor sa efectueze spargerea sistemului:
   - Accesarea informaţiei cu ajutorul deducţiilor logice, potrivirea sau spargerea parolelor utilizatorilor bazei de date, a atacurilor îndreptate spre mărirea prilegiilor în sistem;
   - Agregarea datelor, atacurile de tip SQL injection;
   - Modificarea/înlocuirea datelor etc.
2. *Gestiunea/controlul accesului la SGBD/BD/Server:*
   - Erori şi scăpări din vedere ale personalului de deservire şi a utilizatorilor;
   - Acţiunile lucrătorilor necinstiţi, ofensaţi; acţiunile persoanelor străine;
   - Furtul fizic, distrugerea informaţiei etc.
3. *Atacurile asupra informaţiei care circula în reţea:*
   - Utilizarea conexiunilor existente la baza de date prin reţea, stabilite de utilizatorii autentificaţi;
   - Interceptarea informaţiei în timpul parcurgerii ei prin reţea.
4. *Alte tipuri de atacuri*: asupra sistemului de operare; blocarea accesului către date, supraîncărcarea buferului; hackerii şi virusurii.

Securitatea bazelor de date poate fi asigurată prin intermediul aplicării unor modele care

mai mult sau mai puțin corespund domeniului activității, politicii de securitate, importanței informației organizației.

Un model simplu ar fi compus din 2 elemente: controlul accesului – unde fiecărui utilizator sau proces informațional al sistemului i se atribuie un set de acțiuni permise, pe care le poate efectua în raport cu anumite obiecte; controlul autenticității – realizează dacă utilizatorul sau procesul care încearcă să efectueze o acțiune sau alta este anume acela pe care îl reprezintă.

Un alt model mai sofisticat este acel de multinivel al securității bazei de date, care reprezintă un instrument foarte puternic, însă aduce unele incomodități în ușurința utilizării, productivitate, costuri etc. În așa tipuri de sisteme informația este clasificată în diverse clase de importanță şi, de obicei, se utilizează modelul lui Bell-LaPadula, care gestionează subiecții, procesele, obiectele.

Aplicarea modelelor se poate efectua fie direct în SGBD-ul / baza de date respectivă, fie în sisteme informatice aparte, proiectate şi exploatate în special pentru a asigura protejarea informației.

Metodologii de combatere a riscurilor şi atacurilor asupra bazei de date le putem clasifica în linii mari în 3 categorii:

1. Securitatea bazei de date şi a SGBD – scanarea DB, auditul vulnerabilităților, monitorizarea activităților, controlul accesului.
2. Auditul vulnerabilităților rețelei şi a sistemului de operare – mecanisme bazate pe scanarea rețelei şi exteriorul DB-ului. Rezultatele sunt examinări, rapoarte, determinarea punctelor slabe.
3. Criptarea bazei de date – care include un sistem de management al cheilor ce suporta o varietate de algoritmuri de criptare.

De asemenea, am putea împărți metodele şi după modul de aplicare:

Tehnice:

1. Amplasarea serverelor de BD în segmente de rețea protejate şi securizarea lor.
2. Back-up. Aplicarea tehnologiilor de Cluster Systems. Tirajarea datelor.
3. Utilizarea metodelor eficiente de autentificare (server/OS authentification, parole cu un numar suficient de simboluri, certificate, chei criptate, dispozitive-chei etc.).

Administrative:

1. Standartizarea cu ISO 17799, ISO 27001 (certificarea oficială a sistemelor de securitate informațională).
2. Urmărirea transmiterii informației prin canale de comunicație. Înregistrarea evenimentelor desfăşurate în cadrul SI. Auditul cererilor către SGBD. Înregistrarea activităților utilizatorilor – permite de a omite în unele cazuri potențialele cazuri de

atac asupra bazei de date sau de a investiga încălcările comise deja.

3. Determinarea cazurilor când informaţia nu este utilizată corect.
4. Delimitarea mediilor de administrare şi de dezvoltare.
5. Excluderea cazurilor de integrare a diverselor servicii corporative pe serverul unde e instalat
6. SGBD-ul.
7. Organizarea unei politici eficiente de acordare a drepturilor/rolurilor pentru diverse grupuri de utilizatori. După standartele intenţionale, se disting 3 categorii de roluri: proprietarul informaţiei; răspunzătorul de securitatea informaţiei; cel care utilizează informaţia.

Software:

1. Configurarea mecanismelor proprii de protecţie a bazelor de date (drepturile de acces, privelegiile). Avantaje: precizie, acoperire totală (a scopurilor). Dezavantaje: viteză, complexitate (dimensiuni).
2. În etapa de proiectare să se ia în consideraţie de către proiectanţi/programatori evitarea afişării mesajelor de eroare clienţilor într-un mod care ar putea să divulge unele detalii despre sistem, scheme etc.;
3. Cifrarea bazei de date. Avantaje – un sistem sporit de securitate; dezavantaje: în caz că se defectează serverul sau cade sistemul, e greu de restabilit dacă are nevoie de o aplicaţie în plus care va gestiona cheile, viteza, indexarea.
4. Analiza protecţiei bazelor de date cu ajutorul unor instrumente, aplicaţii, sisteme de audit şi control de acces care pot permite: analiza evenimentelor critice, modelarea acţiunilor răufăcătorilor externi, analiza optimizărilor efectuate în SGBD şi OS, identificarea utilizatorilor necunoscuţi, scanarea centralizată, viziunea asupra securităţii reţelei dintr-o parte etc. şi care pot răspunde la întrebări de tipul: ce baze de date sunt în reţea?; cât de corect e configurat SGBD-ul?, e posibil atacul SGBD-ului dv prin reţea?, corespunde configurarea SGBD-ului dv. cu politica de securitate?, e posibil ca utilizatorii „să înconjoare” mecanismele de protecţie a SGBD-ului şi SO?, care e rezultatul ataşării la SGBD a diverselor mecanisme de protecţie? etc. Dezavantajele acestor tipuri de sisteme sunt: viteza, costurile pentru aplicaţii/computatoare, necoerenţa informaţiei..

Prin urmare, e greu de zis că există 100% de protecţie a informaţiei din baze de date, cel puţin se observă o tendinţă către aceasta. La moment, diversitatea activităţilor organizaţiilor, structura reţelelor şi a fluxulurilor informaţionale nu permite apariţia unor metode universale de soluţii pentru a asigura securitatea bazelor de date.

Bibliografie:

1. http://sr2k.toxahost.ru/Diplom/Proekt.htm
2. http://www.infosec.ru
3. http://citforum.ru/security/articles/
4. http://www.aladdin.ru/catalog/etoken_products/oracle/public_detail.php?ID=7640&phrase_id=82012
5. http://www.rus-lib.ru/book/28/ps/05/396-422.html