



Programul Operațional Capital Uman 2014 - 2020

Axa prioritară 3: Locuri de muncă pentru toți

Obiectivul tematic 3.7: Creșterea ocupării prin susținerea întreprinderilor cu profil non-agricol din zona urbană

Titlu proiect: “**PROMotorii Firmei Tale (PROFIT) – pentru regiunea Centru**” - POCU/82/3.7/104254

Activitatea 6.

Susținerea antreprenoriatului în regiunea de implementare a proiectului

6.3. Studiu de analiză în domeniul antreprenoriatului, bune practici și măsuri de susținere

Bune practici în antreprenoriat

AVANTAJELE CONTROLULUI ACCESULUI ȘI A CLASIFICĂRII DATELOR FOLOSITE ÎN BAZELE DE DATE DIN CADRUL ORGANIZATIILOR IN DOMENIUL FINANCIAR CONTABIL

Autor:

HURLOIU LACRAMIOARA RODICA

Expert bune practici în antreprenoriat

APRILIE 2020





AVANTAJELE CONTROLULUI ACCESULUI ȘI A CLASIFICĂRII DATELOR FOLOSITE ÎN BAZELE DE DATE DIN CADRUL ORGANIZATIILOR IN DOMENIUL FINANCIAR CONTABIL

Creșterea rapidă a cantității și a importanței datelor financiar contabile care sunt colectate și păstrate în baze de date a determinat un interes crescând legat de controlul accesului la date și de clasificarea datelor, reprezentând proceduri foarte importante deoarece orice pierdere a disponibilității datelor, a grupurilor de date sau a pierderii efective a acestora poate constitui o adevărată catastrofă.

Controlul accesului la date urmărește minimizarea pierderile cauzate de diverse evenimente într-o modalitate eficientă din punct de vedere al costurilor, fără a impune utilizatorilor constrângeri insuportabile.

Pe măsură ce organizațiile care au ca obiect de activitate tehnologia informației s-au dezvoltat foarte mult și volumul datelor din diferite domenii acumulat s-a mărit din ce în ce mai mult. Datorită faptului că aceste date pot sta la baza unor decizii foarte importante, au devenit extreme de valoroase pentru organizații, astfel încât este necesar să se acorde mare atenție securității acestora. Drept urmare orice utilizator al bazelor de date din cadrul organizației trebuie atenționat și responsabilizat referitor la breșele de securitate ce pot apărea luându-se măsuri pentru a proteja datele din domeniul în care lucrează.

O dată ce o bază de date a fost securizată, trebuie asigurat faptul că pistele de audit sunt generate și menținute pentru orice activități ale bazei de date care pot avea impact asupra integrității și confidențialității datelor sensitive.

Este absolut necesar ca următoarele trei evenimente să fie auditate:

- Încercări eșuate de logare;
- Încercări reușite de logare;
- Schimbări de configurație.

Dacă este posibil, informația privind activitatea la nivel de interogare a unei baze de date, va furniza o mulțime de date folositoare.





Ca o regulă generală, ultimele trei luni de înregistrare a informațiilor trebuie să fie ușor accesibilă, iar informația mai veche de trei luni poate fi arhivată împreună cu datele și recuperate numai dacă este necesar.

Anual, configurația bazei de date trebuie să fie comparată cu nivelul de referință și orice excepții identificate trebuie să fie documentate și raportate. Excepțiile trebuie să fie clasificate ca schimbări neautorizate sau ca o schimbare autorizată bazată pe o autorizație. Standardele de configurare trebuie să fie actualizate pe măsură ce schimbările sunt făcute, deoarece ele devin parte a bazei de date. Se recomandă realizarea unei revizuirii anuale sau semianuale a drepturilor utilizatorilor.

Securitatea bazelor de date: vedere de ansamblu

De cele mai multe ori, problemele de securitate sunt complexe și pot implica aspecte legale, sociale, sau etice, dar și aspecte legate de politicile implementate sau referitoare la controlul echipamentelor fizice. Securitatea unei baze de date se referă la protecția bazei de date împotriva pericolelor intenționate sau nu, folosind elemente de control ce pot fi sau nu bazate pe echipamente de calcul.

Analiza securității unei baze de date nu include doar serviciile oferite de sistemul de gestiune al bazei de date, dar și o serie de aspecte asociate bazei de date și securității mediului.

Aspectele legate de securitate nu se referă doar la datele existente în baza de date, deoarece breșele de securitate pot afecta și alte părți ale sistemului, care, ca rezultat, pot afecta baza de date.

Drept urmare dacă atenția este concentrată doar asupra securității bazei de date nu se va obține o bază de date sigură. Toate componentele sistemului trebuie să fie sigure: baza de date, rețeaua, sistemul de operare, clădirea în care se află baza de date, dar și persoanele care accesează sistemul. O vedere de ansamblu asupra securității unei baze de date este ilustrată în *Figura 1*.



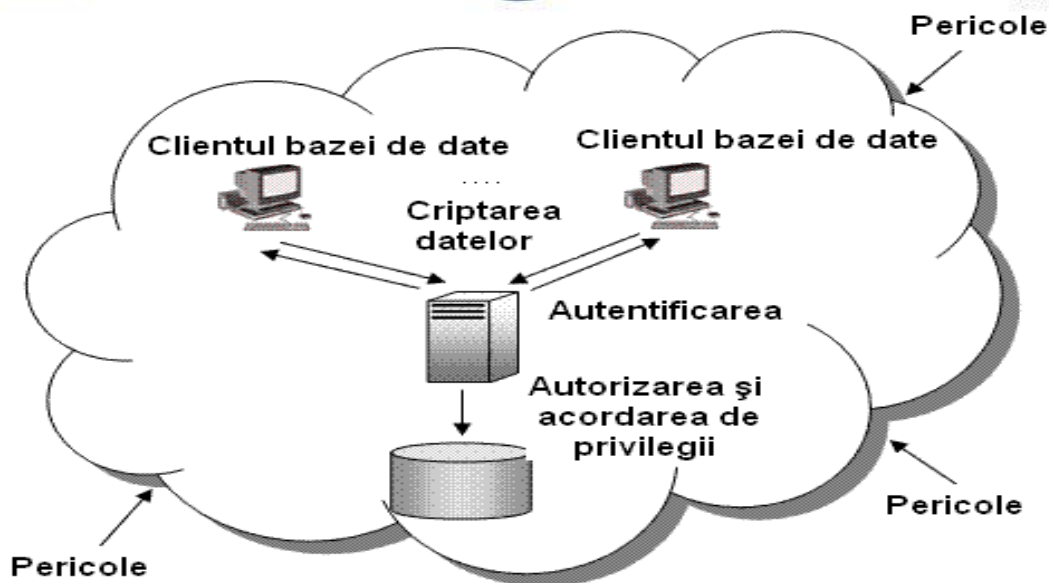


Figura 1 – Securitatea bazei de date

Sursa: Baze de date-Fundamente, Neeraj Sharma, Liviu Perniu si colectivul, 2010

În procesul de proiectare și implementare a unei baze de date sigure se urmărește atingerea următoarelor obiective:

- Caracterul privat reflectat în faptul că datele nu pot fi cunoscute de persoane neautorizate;
- Integritatea - datele pot fi modificate doar de către utilizatorii autorizați;
- Disponibilitatea - utilizatorilor autorizați nu le este interzis accesul;

Pentru atingerea acestor obiective, trebuie să se elaboreze o politică de securitate în care să se facă referire la măsurile ce trebuie impuse. În particular, trebuie determinați utilizatorii care pot accesa baza de date precum și datele la care aceștia au acces. Pentru o mai bună securitate a bazei de date trebuie stabilite și operațiile permise pe clasa de date.

De asemenea se poate apela la mecanismul de securitate oferit de către sistemul de gestiune al bazei de date și/sau la cel oferit de către sistemul de operare. Persoanele responsabile cu securitatea bazelor de date sunt numite administratori de baze de date și trebuie să aibă în vedere diversele pericole care pândesc sistemul.



Administratorii bazelor de date stabilesc regulile de autorizare prin care se stabilesc celelalte persoane care vor avea acces la baza de date, care parte a acesteia poate fi accesată de către ce utilizator, precum și operațiile permise acestora.

Motivul pentru care securitatea unei baze de date a devenit un aspect atât de important este acela al creșterii cantității și importanței cruciale a datelor care sunt colectate și păstrate pe sistemele de calcul. Orice pierdere a disponibilității datelor sau a pierderii efective a acestora poate avea dimensiuni catastrofice. O bază de date reprezintă o resursă colectivă esențială care trebuie asigurată în mod adecvat, folosind elementele de control cele mai potrivite.

Securitatea bazei de date își propune să minimizeze pierderile cauzate de evenimentele amintite anterior într-o modalitate eficientă din punct de vedere al costurilor, fără a impune utilizatorilor constrângeri insuportabile. Deoarece criminalitatea pe calculator este în plină expansiune, iar acest tip de infracțiuni poate amenința toate componentele unui sistem, introducerea de măsuri de securitate adecvate devine vitală.

Cele mai folosite măsuri ce se pot lua pentru a asigura protecția și integritatea datelor sunt: controlul accesului, folosirea vederilor, controlul integrității și criptarea. Este de asemenea necesar să se stabilească cele mai adecvate politici și proceduri de securitate care se referă la personal și la controlul fizic al accesului.

Controlul accesului la datele din baze de date

O primă idee de cercetare s-a axat pe inferența datelor sensibile în bazele de date statistice. Principala metodă utilizată pentru a proteja datele este de a limita accesul la date.

Acest lucru poate fi realizat prin autentificare, autorizare și control accesului utilizatorilor la obiectele specifice.

Aceste trei mecanisme sunt distinct diferite dar, de obicei, sunt folosite în combinație, cu accent pe controlul accesului pentru acordarea drepturilor.

De exemplu, majoritatea sistemelor de baze de date utilizează o formă de autentificare cum ar fi nume de utilizator și o parolă, pentru a restricționa accesul la sistem sau pentru a atribui privilegii definite la resursele specifice. Controlul accesului, în continuare, rafinează procesul prin atribuirea de drepturi și privilegii pentru obiectele de date specifice și seturi de date.





În cadrul unei baze de date, aceste obiecte includ, de obicei, tabele, vizualizări, rânduri și coloane de bază. În controlul accesului au fost propuse modele pentru a restricționa accesul pentru utilizatori pe baza privilegiului de utilizatori.

La baza controlului accesului se găsesc două premise:

– identificarea corectă a utilizatorului

• asigurată prin autentificare

• nici un utilizator să nu poată lua drepturile de acces ale altui utilizator

– informația despre drepturile de acces este protejată contra modificărilor neautorizate

Se pune problema dreptului de acces a, a subiectului s, la obiectul o.

– Tuplul (s, o, a) constituie “autorizația”

– Controlul accesului reprezentând funcția logică $f(s, o, a)$ care întoarce true sau false.

Controlul accesului este un sistem care face posibil ca o autoritate să controleze accesul într-o arie, sau a resurselor într-o grădiniță fizică dată, sau într-un sistem informatic.

Controlul accesului este în realitate un fenomen ce se petrece zilnic. Controlul unui element sau managementul electronic al cheii este o arie în cadrul unui sistem de control al accesului care privește gestionarea posesiei și locației activelor mici și cheilor fizice.

Controalele electronice de acces folosesc calculatoarele pentru a rezolva limitările încuietorilor mecanice și a cheilor. O largă gamă de parole pot fi folosite pentru a înlocui cheile mecanice. Controlul accesului electronic acordă acces bazat pe date de identificare. Când accesul este acordat, ușa este deschisă pentru un timp predeterminat iar tranzacțiile sunt înregistrate. Când accesul este refuzat, ușa rămâne închisă și încercarea de acces este înregistrată. Sistemul va monitoriza de asemenea ușa și alarma; dacă ușa este deschisă forțat sau ținută prea mult deschisă după ce a fost deblocată.

În securitatea calculatoarelor, controlul accesului include autentificarea, autorizarea și auditul. Pe lângă aceste procese mai include și măsuri cum ar fi: dispozitive fizice, incluzând încuietori mecanice, căi ascunse, semnături digitale, încriptare, bariere sociale și monitorizare de sisteme umane și automate.

În orice model de control al accesului, entitățile care pot să realizeze acțiuni în cadrul sistemului sunt numiți subiecți, iar entitățile reprezentând resursele la care este necesar ca





accesul sa fie controlat sunt numite obiecte. Subiectele și obiectele trebuie să fie ambele considerate ca entități software și ca utilizatori umani.

Identificarea și autentificarea reprezintă procesul de verificare a unei identități dacă este legată de entitatea care face afirmația ori pretinde identitatea. Procesul de identificare și autentificare presupune că a existat o validare inițială a identității, de obicei denumită dovada identității. Diferite metode de dovadă a identității sunt disponibile variind de la validarea personală la metode anonime care permit solicitantului să rămână anonim, dar cunoscut sistemului dacă el se întoarce. Metoda utilizată pentru dovada identității și validării ar trebui să asigure un nivel de siguranță corespunzător cu intenția de utilizare a identității în cadrul sistemului. Ulterior entitatea afirmă o identitate împreună cu un autentificator ca un mijloc de validare. Singura cerință pentru identificator este că trebuie să fie unic în cadrul domeniului său de securitate.

Autentificatorii sunt în mod comun bazați pe cel puțin unul din următorii patru factori:

- Ceva ce se cunoaște, cum ar fi o parolă sau un număr personal de identificare. Aceasta presupune că numai posesorul contului cunoaște parola sau PIN-ul necesar pentru a accesa contul.

- Ceva ce există, cum ar fi un smart card sau security token. Aceasta presupune că numai posesorul contului are smart card-ul sau token-ul necesar pentru a debloca contul.

- Ceva ce reprezintă subiectul, cum ar fi amprente, vocea, retina sau caracteristicile irisului.

- Unde se găsește, de exemplu în interiorul sau exteriorul firewall-ului companiei, sau proximitatea locației de logare pentru un dispozitiv personal GPS.

Autorizația se aplică subiecților. Autorizarea determină ce poate un subiect să facă în cadrul sistemului.

Majoritatea sistemelor de operare moderne definesc seturi de permisiuni care sunt variații sau extensii a trei tipuri de acces de bază:

- Citire (R): Subiectul poate să citească conținutul fișierului sau să citească lista conținutului directorului.
- Scriere (W): Subiectul poate modifica conținutul unui fișier sau directorul prin următoarele sarcini: adăugare, creere, ștergere, redenumire.





- Executare (X): Dacă fișierul este un program, subiectul poate determina rularea programului.

Aceste drepturi și permisiuni sunt implementate în mod diferențiat în sistemele bazate pe un control al accesului discreționar (Discretionary Access Control DAC) și control al accesului obligatoriu Mandatory Access Control (MAC).

Responsabilitatea folosește asemenea componente de sistem cum ar fi pistele de audit și înregistrări pentru a asocia un utilizator cu acțiunile sale. Informația înregistrată trebuie să fie suficientă pentru a mapa subiectul la un controlling user.

Pistele de audit și înregistrările sunt importante pentru:

- Detectarea violărilor de securitate;
- Recrearea incidentelor de securitate;
- Dacă nimeni nu revizuieste înregistrările utilizatorului în mod constant și ele nu sunt menținute într-o manieră securizată și consistentă, ele nu pot fi admise ca probe.
- Multe sisteme pot genera rapoarte automate bazate pe anumite criterii predefinite sau praguri cunoscute ca clipping levels.

De exemplu, un clipping level poate fi setat pentru a genera un raport pentru următoarele:

- mai mult de trei încercări eșuate de logare într-o anumită perioadă;
- orice încercare de utilizare a unui cont dezactivat;

Aceste rapoarte ajută un administrator de sistem sau un administrator de securitate pentru a identifica mai ușor încercările de pătrundere în sistem.

Referitor la controlul accesului, în practică se cunosc două concepte importante referitoare la securitatea datelor și anume: *control discreționar* și *control obligatoriu*. În ambele situații, datele sau grupurile de date care trebuie protejate poate să conțină întreaga bază de date sau doar câteva rânduri. Prin conceptul controlului discreționar, utilizatorul va avea diferite drepturi de acces, cunoscute sub denumirea de privilegii acordate pe anumite date, grupuri de date sau obiecte. Bineînțeles există o serie de limitări din punct de vedere al drepturilor pe care un utilizator le are asupra unui anumit obiect.

Dacă este implementat conceptul controlului discreționar, un utilizator poate avea acces la obiectul α din baza de date, dar nu poate avea acces la obiectul β , în timp ce alt utilizator poate accesa obiectul β , dar nu poate accesa obiectul α .





Schemele de control discreționar sunt foarte flexibile datorită faptului că se pot combina drepturile atribuite utilizatorilor și obiectelor în funcție de necesități.

Dacă vorbim de controlul obligatoriu atunci fiecărui obiect sau dată îi este asociat unui anumit nivel de clasificare iar fiecărui utilizator i se atribuie un anumit nivel de permisiuni. Orice obiect sau dată poate fi accesat doar de către utilizatorii care au permisiunile corespunzătoare. Schemele obligatorii sunt mult mai rigide decât cele discreționare deoarece acestea sunt de tip ierarhic. În funcție de tipul de schemă de securitate care se folosește, toate deciziile referitoare la drepturile pe care le au diverși utilizatori asupra obiectelor din baza de date sunt decizii ce depind de domeniul de care aparțin, nu sunt decizii tehnice.

Pentru a decide care sunt constrângerile de securitate aplicabile unei cereri de acces, sistemul trebuie să poată recunoaște sursa cererii. Cu alte cuvinte, trebuie să recunoască utilizatorul care a lansat în execuție aplicația și trebuie să verifice drepturile pe care le are acesta.

Strategii de clasificare a datelor

Clustering sau gruparea datelor este o metodă de a analiza date obținute prin măsurători. Această tehnică este utilă atunci când se lucrează cu cantități mari de date, ceea ce nu este neîntâlnit dacă ținem cont de explozia de date și informații din zilele noastre.

Clustering este un proces care examinează o colecție de date și le grupează în clustere, grupepe baza unor măsurători ale distanței. Scopul principal al procesului de clustering, grupare, este de a obține o stare în care punctele din același cluster să aibă o distanță mică unul față de altul, iar punctele din grupe diferite să fie la o distanță mare unele de altele.

Aprecierea distanței ca fiind mică sau mare depinde de domeniul în care se aplică gruparea. Se cunosc două tipuri de strategii de clustering: algoritmi ierarhici și algoritmi de atribuire a punctelor.

Algoritmii ierarhici încep cu fiecare punct în propriul său cluster, combină clusterii în funcție de diferitele definiții de apropiere și se oprește atunci când combinații suplimentare ar duce la formarea unor clustere indezirabile, cum ar fi atunci când am ajuns la un număr predeterminat de clustere pentru un anumit domeniu sau când un cluster rezultat are puncte ce se întind pe o suprafață mult prea mare.





În algoritmi de atribuire a punctelor, punctele sunt luate în considerare într-o anumită ordine și fiecare dintre ele este atribuit cluster-ului în care se potrivește cel mai bine. Aceasta este de obicei precedată de o fază scurtă în care se estimează clusterelor inițiale. Ocazional, variații ale acestor algoritmi combină sau separă clusterelor sau permit punctelor să fie dezatribuite, dacă acestea se află prea departe de oricare dintre clusterelor actuale, pentru a reduce zgomotul. Atunci când bazele de date conțin cantități uriașe de date și se urmărește analiza și organizarea datelor în spații supra-dimensionale este foarte des întâlnită denumirea de “blestemul” dimensionalității. Problema principală în astfel de cazuri este că pe măsură ce dimensionalitatea crește și volumul spațiului se mărește foarte repede astfel încât datele disponibile devin împrăștiate. Acest lucru este critic pentru orice metodă în care este nevoie de relevanță statistică. Astfel, în ceea ce privește partea statistică, pentru a obține un rezultat corect și de încredere, cantitatea de date necesară pentru a susține rezultatul crește deseori exponențial cu dimensionalitatea.

Concluzii

Dacă asigurarea securității este îndreptată numai asupra bazei de date atunci nu se va obține o bază de date sigură. Pentru a se atinge acest obiectiv trebuie urmărit ca, pe lângă baza de date și celelalte componente ale sistemului să fie sigure: rețeaua, sistemul de operare, clădirea în care se află baza de date financiar contabilă, cât și persoanele care accesează sistemul.

Clasificarea datelor ne permite gruparea datelor în clase și are avantajul de a utiliza clasele obținute drept bază în învățarea automată. Totodată aceasta oferă analiza mai rapidă a măsurătorilor sau valori aproximative ale unor măsurători viitoare, prin extrapolare.

