Programul Operaţional 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 implemenatre a proiectului

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

Bune practici în antreprenoriat

CONTROLUL ACCESULUI ŞI CLASIFICAREA DATELOR FOLOSITE ÎN BAZELE DE DATE DIN CADRUL ORGANIZAȚIILOR

Autor:

HURLOIU LĂCRĂMIOARA RODICA

Expert bune practici în antreprenoriat

Iunie, 2019

Proiect cofinanțat din Fondul Social European prin Programul Operațional Capital Uman

CONTROLUL ACCESULUI ŞI CLASIFICAREA DATELOR FOLOSITE ÎN BAZELE DE DATE DIN CADRUL ORGANIZAȚIILOR

Pe măsură ce organizaţiile care au ca obiect de activitate tehnologia informaţiei s-au dezvoltat foarte mult şi 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 organizaţii, astfel încât este necesar să se acorde mare atenţie securităţii acestora. Drept urmare orice utilizator al bazelor de date din cadrul organizaţiei trebuie atenţionat şi responsabilizat referitor la breşele de securitate ce pot apare 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 şi menţinute pentru orice activităţi ale bazei de date care pot avea impact asupra integrităţii şi confidenţialităţii datelor sensitive.

Este absolut necesar ca urmatoarele trei evenimente să fie auditate:

- Încercări eşuate de logare;
- Încercări reuşite de logare;
- Schimbări de configuraţie.

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

Ca o regulă generală, ultimele trei luni de înregistrare a informaţiilor trebuie să fie uşor accesibilă, iar informaţia mai veche de trei luni poate fi arhivată împreuna cu datele şi recuperate numai dacă este necesar.

Anual, configuraţia bazei de date trebuie sa fie comparată cu nivelul de referinţă şi orice excepţii identificate trebuie să fie documentate şi raportate. Excepţiile trebuie să fie clasificate ca schimbări neautorizate

sau ca o schimbare autorizată bazată pe o autorizaţie. Standardele de configurare trebuie sa fie actualizate pe masură ce schimbările sunt făcute, deoarece ele devin parte a bazei de date. Se recomandă realizarea unei revizuiri anuale sau semianuale a drepturilor utilizatorilor.

Securitatea bazelor de date: vedere de ansamblu

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

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

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

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

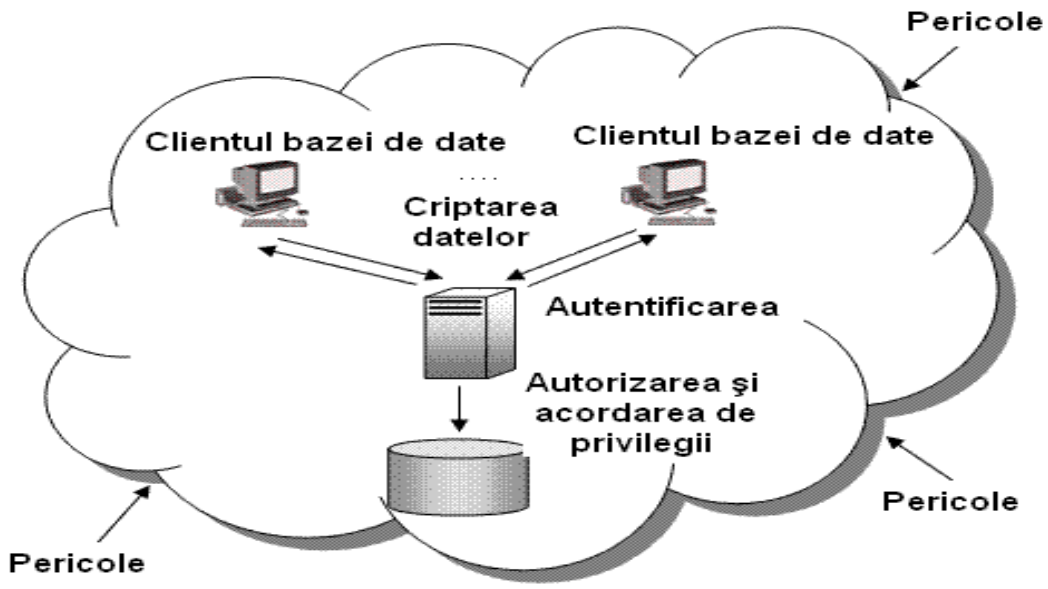

Figura 1 – Securitatea bazei de date

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

În procesul de proiectare şi implementare a unei baze de date sigure se urmăreşte atingerea următoarelor obiective:

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

Pentru atingerea acestor obiective, trebuie să se eleboreze o politică de securitate în care să se facă referire la măsurile ce trebuie impuse. În particular, trebuie determinaţi utilizatorii care pot accesa baza de date precum şi datele la care aceştia au acces. Pentr trebuieu o mai bună securitate a bazei de date trebuie stabilite şi operaţiile permise pe clasa de date.

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

Administratori 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 şi operaţiile permise acestora.

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

Securitatea bazei de date îşi 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 infracţiuni poate ameninţa toate componentele unui sistem, introducerea de măsuri de securitate adecvate devine vitală.

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

Controlul accesului la datele din baze de date

O primă idee de cercetare s-a axat pe inferenţa 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 şi control accesului utilizatorilor la obiectele specifice.

Aceste trei mecanisme sunt distinct diferite dar, de obicei, sunt folosite în combinaţie, 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 şi o parolă, pentru a restricţiona accesul la sistem sau pentru a atribuii privilegii definite la resursele specifice. Controlul accesului, în continuare, rafinează procesul prin atribuirea de drepturi şi privilegii pentru obiectele de date specifice şi seturi de date.

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

– informaţia 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 "autorizaţia"

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

Controlul accesului este un sistem care face posibil ca o autoritate sa controleze accesul într-o arie, sau a resurselor într-o gracilitate 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 priveşte gestionarea posesiei şi locaţiei activelor mici şi cheilor fizice.

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

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

În orice model de control al acesului, entităţile care pot să realizeze acţiuni în cadrul sistemului sunt numiţi subiecţi, iar entităţile reprezentând

resursele la care este necesar ca accesul sa fie controlat sunt numite obiecte. Subiectele şi obiectele trebuie să fie ambele considerate ca entităţi software şi ca utilizatori umani.

Identificarea şi autentificarea reprezintă procesul de verificare a unei identităţi dacă este legată de entitatea care face afirmaţia ori pretinde identitatea. Procesul de identificare şi autentificare presupune că a existat o validare iniţială a identităţii, de obicei denumită dovada identităţii. Diferite metode de dovadă a identităţii sunt disponibile variind de la validarea personală la metode anonime care permit solicitanului să ramână anonim, dar cunoscut sistemului dacă el se întoarce. Metoda utilizată pentru dovada identităţii şi validarii ar trebui să asigure un nivel de siguranţă corespunzator cu intenţia de utilizare a identităţii în cadrul sistemului. Ulterior entitatea afirmă o identitate împreună cu un autentificator ca un mijloc de validare. Singura cerinţă pentru identificator este că trebuie să fie unic în cadrul domeniului său de securitate.

Autentificatorii sunt în mod comun bazaţi pe cel puţin unul din următorii patru factori:

- Ceva ce se cunoaşte, cum ar fi o parola sau un numar personal de identificare. Aceasta presupune că numai posesorul contului cunoaşte 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 smat card-ul sau token-ul necesar pentru a debloca contul.

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

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

Autorizaţia se aplica subiecţilor. Autorizarea determină ce poate un subiect sa facă în cadrul sistemului.

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

- Citire (R): Subiectul poate să citească conţinutul fişierului sau să citească lista conţinutului directorului.
- Scriere (W): Subiectul poate modifica conţinutul unui fişier sau directorul prin următoarele sarcini: adăugare, creere, ştergere, redenumire.
- Executare (X): Dacă fişierul este un program, subiectul poate determina rularea programului.

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

Responsabilitatea foloseşte asemenea componente de sistem cum ar fi pistele de audit şi înregistrări pentru a asocia un utilizator cu acţiunile sale. Informaţia înregistrată trebuie să fie suficientă pentru a mapa subiectul la un controlling user.

Pistele de audit şi înregistrările sunt importante pentru:

- Detectarea violărilor de securitate;
- Recreerea incidentelor de securitate;
- Dacă nimeni nu revizuieşte înregistrările utilizatorului în mod constant şi ele nu sunt menţinute într-o maniera securizată şi 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 urmatoarele:

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

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

Referitor la controlul accesului, în practică se cunosc două concepte importante referitoare la securitatea datelor şi anume: *control discreţionar* şi *control obligatoriu*. În ambele situaţii, datele sau grupurile de date care trebuie protejeate poate să conţină întreaga bază de date sau doar câteva rânduri. Prin conceptul controlului discreţionar, utilizatorul va avea diferite drepturi de acces, cunoscute sub denumirea de privilegii acordate pe anumite date, grupuri de date sau obiecte. Bineînteles 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 discreţionar, 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 discreţionar sunt foarte flexibile datorită faptului că se pot combina drepturile atribuite utilizatorilor şi obiectelor în funcţie de necesităţi.

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 discreţionare deoarece acestea sunt de tip ierarhic. În funcţie de tipul de schemă de securitate care se foloseşte, toate deciziile referitoare la drepturile pe care le au diverşi utilizatori asupra obiectelor din baza de date sunt decizii ce depind de domeniul de care aparţin, nu sunt decizii tehnice.

Pentru a decide care sunt constrângerile de securitate aplicabile unei cereri de acces, sistemul trebuie să poată recunoaşte sursa cererii. Cu alte cuvinte, trebuie să recunoască utilizatorul care a lansat în execuţie aplicaţia şi trebuie să verifice drepturile pe care la are acesta.

Strategii de clasificăre a datelor

Clustering sau gruparea datelor este o metodă de a analiza date obţinute prin măsurători. Această tehnică este utilă atunci când se lucrează cu cantităţi mari de date, ceea ce nu este neîntâlnit dacă ţinem cont de explozia de date şi informaţii din zilele noastre.

Clustering este un proces care examinează o colecţie de date şi le grupează în clustere, grupepe baza unor măsurători ale distanţei. Scopul principal al procesului de clustering, grupare, este de a obţine o stare în care punctele din acelaşi cluster să aibă o distanţă mică unul faţă de altul, iar punctele din grupe diferite să fie la o distanţă mare unele de altele.

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

Algoritmii ierarhici încep cu fiecare punct în propriul său cluster, combină clusterii în funcţie de diferitele definiţii de apropiere şi se opreşte atunci când combinaţii 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 suprafaţă mult prea mare.

În algoritmii de atribuire a punctelor, punctele sunt luate în considerare într-o anumită ordine şi fiecare dintre ele este atribuit cluster-ului în care se potriveşte cel mai bine. Aceasta este de obicei precedată de o fază scurtă în care se estimează clusterele iniţiale. Ocazional, variaţii ale acestor algoritmi combină sau separă clusterele sau permit punctelor să fie dezatribuite, dacă acestea se află prea departe de oricare dintre clusterele actuale, pentru a reduce zgomotul. Atunci când bazele de date conţin cantităţi uriaşe de date şi se urmăreşte analizarea şi organizarea datelor în spaţii supra-dimensionale este foarte des întâlnită denumirea de "blestemul" dimensionalităţii. Problema principală în astfel de cazuri este că pe măsură ce dimensionalitatea creşte şi volumul spaţiului se măreşte foarte repede astfel încât datele disponibile devin împrăştiate. Acest lucru este critic pentru orice metodă în care este nevoie de relevanţă statistică. Astfel, în ceea ce priveşte partea statistică, pentru a obţine un rezultat corect şi de încredere, cantitatea de date necesară pentru a susţine rezultatul creşte deseori exponenţial cu dimensionalitatea.

Concluzii

Dacă asigurarea securităţii este îndreptată numai asupra bazei de date atunci nu se va obţine o bază de date sigură. Pentru a se atinge acest obiectiv trebuie urmărit ca, pe lângă baza de date şi celelalte component ale sistemului să fie sigure: reţeaua, sistemul de operare, clădirea în care se află baza de datefinanciar contabilă, cât şi persoanele care accesează sistemul.

Clasificarea datelor ne permite gruparea datele în clase şi are avantajul de a utiliza clasele obţinute drept bază în învăţarea automată. Totodată aceasta oferă analizarea mai rapidă a măsurătorilor sau valori aproximative ale unor măsurători viitoare, prin extrapolare.