

Access Control in Data Management Systems

[Controlul accesului în sistemele de gestiune a datelor]

Liliana COJOCARU¹

¹ Associate Professor Ph.D., "Petre Andrei" University of Iași, Romania, e-mail: lcojocarus@yahoo.com

Mircea Răzvan BRINDA¹

¹ Undergraduate student, "Petre Andrei" University of Iași, Romania.

Abstract

An access control system is a collection of rules used to restrict the visibility, access, and usage of the data resources in an institutional environment. When implemented, these rules provide a policy for achieving the security of the institution, establishing a hierarchy of the employees depending on their rights over the institution's data resources. An access control system is based on two fundamental concepts: authentication (that verifies the user's identity) and authorization (that provides a hierarchy of the employees according to their access rights over the institutional resources). Among the most commonly used access control models we recall Role-Based Access Control (RBAC), in which users with the same role have equal access rights to data resources, Discretionary Access Control (DAC), in which the system owner decides which user has access to system resources, and Mandatory Access Control (MAC), in which a series of rules, with a high level of security established by a predefined authority, are used. In this article, we will study the last two models, namely DAC and MAC, along with their main implementations: Access Control Matrix and the Take-Grant models for DAC, BIBA and Bell-LaPadula for MAC.

Keywords: RBAC; DAC; MAC; Access Control Matrix; Take-Grant; Bell-LaPadula; BIBA.

How to cite: Cojocaru, L., & Brinda, M.R. (2026). Access Control in Data Management Systems. *Anuarul Universității "Petre Andrei" din Iași, Fascicula: Drept, Științe Economice, Științe Politice*, 36, 135-146.
<https://doi.org/10.63331/upalaw/36/13>

1. Introducere - Context și motivație

În era digitală actuală, securitatea informațiilor reprezintă una dintre principalele preocupări ale organizațiilor moderne. Sistemele de control al accesului constituie prima linie de apărare atât împotriva amenințărilor cibernetice, cât și împotriva accesului neautorizat la datele sensibile ale organizațiilor. Un sistem de control al accesului¹ poate fi definit ca un ansamblu de tehnici, politici și proceduri care reglementează accesul utilizatorilor la resursele informatice ale unei organizații. Aceste sisteme funcționează pe o serie de principii de securitate, asigurându-se că fiecare utilizator are acces doar la informațiile necesare pentru îndeplinirea sarcinilor sale profesionale. Controlul accesului se bazează pe două concepte fundamentale care formează baza oricărui sistem de securitate, anume *Autentificarea* și *Autorizarea*.

Autentificarea reprezintă procesul de verificare a identității unui utilizator. Acest proces confirmă că utilizatorul este cine pretinde că este, prin intermediul credențialelor furnizate (parole, carduri, biometrie etc.). Autentificarea răspunde la întrebarea „Cine ești?”.

Autorizarea reprezintă procesul de determinare a drepturilor și permisiunilor unui utilizator autentificat. După ce identitatea utilizatorului a fost confirmată, sistemul determină ce resurse poate accesa și ce operații poate efectua asupra acestor resurse. Autorizarea răspunde la întrebarea „Ce drepturi ai?”.

În cadrul acestui articol, vom analiza principalele modele de control al accesului, cu accent pe modelele *DAC (Discretionary Access Control)* și *MAC (Mandatory Access Control)*. Vom examina implementările specifice ale acestor modele, precum *Matricea de Control al Accesului* și *Modelul Take-Grant* pentru DAC, respectiv modelele *BIBA* și *Bell-LaPadula* pentru MAC. De asemenea, vom prezenta un studiu de caz practic care exemplifică implementarea unui sistem de control al accesului la o companie fictivă de monitorizare a securității instituționale.

Articolul este organizat astfel: în *Secțiunea 1* prezentăm o scurtă introducere în care sunt amintite conceptele de bază și metodologiile folosite pe parcursul articolului, împreună cu descrierea succintă a structurii lucrării. În *Secțiunea 2* prezentăm principalele modele de control al accesului, anume RBAC, DAC și MAC, împreună cu o succintă descriere a acestora. În *Secțiunea 3* abordăm principalele implementări ale modelului DAC, anume Matricea de Control al Accesului și Modelul Take-Grant. În *Secțiunea 4* abordăm principalele implementări ale modelului MAC, anume BIBA și Bell-LaPadula. În *Secțiunea 5* realizăm un studiu de caz asupra implementării controlului accesului pentru o companie fictivă GPS SECURITY SRL, operator de sisteme de securitate pentru instituții publice.

2. Principalele Modele de Control al Accesului

2.1. Role-Based Access Control (RBAC)

RBAC (Controlul accesului bazat pe roluri) este unul din cele mai răspândite modele de control al accesului în organizațiile moderne. În acest model, drepturile de acces sunt acordate pe baza rolurilor pe care utilizatorii le dețin în cadrul organizației și nu direct pe baza identității individuale.

¹ Maria Penelova, "Access Control Models", in *Cybernetics and Information Technologies*, Vol. 21(4), 2021, pp. 77-104.

Componentele principale ale modelului RBAC² sunt *Utilizatorii* – persoanele care accesează sistemul, *Rolurile* – funcțiile sau pozițiile ocupate în cadrul organizației (manager, contabil, operator), *Permișiunile* – drepturile de acces la resurse (citire, scriere, ștergere) și *Sesiunile* – mapări dinamice între utilizatori și rolurile active.

Principalele avantaje ale acestui model sunt simplitatea administrativă, flexibilitatea organizațională (pe măsura ce apar noi cerințe, noi roluri pot fi create), separarea responsabilităților (utilizatorii cu același rol au aceleași drepturi de acces) și ușurința în audit. Totuși, simplitatea administrativă poate conduce și la o serie de dezavantaje, precum dificultăți în gestionarea cazurilor de risc sau în preluări excesive de roluri în cazul organizațiilor mari.

2.2. Discretionary Access Control (DAC)

DAC (*Controlul Accesului Discreționar*) este un model³ în care proprietarul unei resurse are controlul complet asupra modului în care aceasta este accesată. Proprietarul poate decide în mod discreționar (la propria discreție) care utilizatori pot accesa resursa și ce operații pot efectua. Acesta este singurul care poate transmite permisiuni asupra resurselor proprii unui alt utilizator.

Principalele caracteristici ale acestui model sunt *Flexibilitatea* – proprietarul poate modifica permisiunile oricând, *Autonomia* – fiecare utilizator controlează propriile resurse, și *Propagarea drepturilor* – utilizatorii pot transfera oricând drepturi către alți utilizatori.

Modelul devine avantajos datorită flexibilității implementării acestuia în practică. Prezintă însă și o serie de dezavantaje majore, precum risc de securitate mărit prin propagarea necontrolată a drepturilor utilizatorilor, este dificil de auditat și este vulnerabil la atacuri cibernetice.

2.3. Mandatory Access Control (MAC)

MAC (*Controlul obligatoriu al accesului*) este un model non-discreționar, strict centralizat în care accesul la resurse este controlat de o autoritate centrală pe baza unor reguli stricte (acțiuni pe care un subiect le poate efectua asupra unui obiect). Un *subiect* poate fi un utilizator sau un proces. Un *obiect* poate fi un fișier, un port sau un dispozitiv de intrare/ieșire. Utilizatorii individuali nu pot modifica politicile de acces, indiferent de statutul lor de proprietari ai resurselor. Modelul⁴ este folosit în special în organizații cu un grad mare de ierarhizare pe niveluri de complexitate și securitate.

Principalele caracteristici ale acestui model sunt *Controlul centralizat* – toate deciziile sunt luate de administratorul de sistem, *Clasificarea obligatorie* – toate resursele și utilizatorii au etichete de securitate, existența *Regulilor stricte* – accesul se acordă doar dacă sunt îndeplinite anumite condiții.

Modelul este avantajos datorită faptului că oferă o securitate ridicată, un control centralizat, previne scurgerile de informații și este ideal pentru instituții militare sau guvernamentale. Printre principalele dezavantaje ale modelului amintim lipsa flexibilității, costurile administrative ridicate și complexitatea implementării.

² Ravi Sandhu, "Role-based Access Control", in *Advances in Computers*, Vol. 46, 1998, pp. 237- 286.

³ Ravi Sandhu, Qamar Munawer, "How to do Discretionary Access Control Using Roles", in *Proceedings of the 3rd ACM Workshop on Role-Based Access Control*, 1998, pp. 17-54.

⁴ Carl Landwehr, Constance Heitmeyer, John Mclean, "A Security Model for Military Message Systems", in *ACM Transactions on Computer Systems*, Vol. 2(3), August 1984, pp. 198-222.

3. Implementările Modelului DAC

3.1. Matricea de Control al Accesului

Matricea de Control al Accesului (Access Control Matrix) ⁵ este cea mai simplă și intuitivă implementare a modelului DAC. Reprezintă o structură tabelară bidimensională care mapează relațiile dintre subiecți (utilizatori) și obiecte (resurse). Într-o astfel de matrice liniile reprezintă subiecții (utilizatori, procese) iar coloanele reprezintă obiectele (fișiere, baze de date, resurse). Celulele matricii vor conține drepturile de acces ale utilizatorilor asupra obiectelor. Aceste drepturi pot fi: *read* – *r* (dreptul de citire), *write* – *w* (dreptul de scriere), *execute* – *e* (dreptul de a executa un program), *own* – *o* (dreptul de a modifica permisiunile). Sistemul permite o serie de operații „primitive” precum adăugarea (*enter r into*) sau ștergerea (*delete r from*) unui drept *r* (al unui subiect asupra unui obiect), crearea unui subiect (*create subject*) sau obiect (*create object*), eliminarea unui subiect (*destroy subject*) sau obiect (*destroy object*).

Pentru exemplificare, în Matricea de Control din Figura 1 Alice are drepturile de read, write și own asupra Fișierului A, are doar dreptul de read asupra fișierului B și drepturile de read și write asupra Bazei de Date.

Utilizator	Fișier_A	Fișier_B	Baza_Date
Alice	r, w, o	r	r, w
Bob	r	r, w, o	r
Carol	-	r	r, w, e, o

Figura 1. Matricea de control al accesului pentru modelul DAC.

Implementarea modelului DAC prin matrici de control este avantajoasă datorită simplității acestei structuri, fiind ușor de înțeles și vizualizat, datorită modului în care sunt centralizate drepturile utilizatorilor (într-o singură celulă) și datorită flexibilității structurii (orice combinație de permisiuni este posibilă). Printre principalele dezavantaje ale acestei implementări amintim: scalabilitatea redusă (matricea devine foarte mare pentru organizații cu mulți utilizatori și resurse), stocarea ineficientă (multe celule rămân nealocate), dificultăți în actualizare (modificările necesită parcurgerea întregii matrici). În practică, matricea de control este implementată folosind Access Control Lists (ACLs) pentru eficiență în stocare și căutare rapidă.

3.2. Modelul Take-Grant

Modelul Take-Grant este o reprezentare dinamică bazată pe teoria grafurilor, care descrie modul în care drepturile de acces pot fi transferate între utilizatorii unui sistem. Spre deosebire de matricea (statică) de control, acest model captează natura dinamică a

⁵ Gregory Saunders, Michael Hitchens, Vijay Varadharajan, "Role-Based Access Control and the Access Control Matrix", in *Proceedings of the 5th International Conference on Information and Communications Security*, 2003, pp. 145-157.

propagării drepturilor. Modelul de protecție Take-Grant⁶ este compus dintr-un set de subiecți (utilizatori sau procese) și obiecte (resurse, directoare, fișiere), un set de reguli de tranziție și un graf orientat (digraf) care implementează aceste reguli. Nodurile din acest digraf reprezintă subiecții și obiectele modelului. Muchiile orientate dintre noduri reprezintă drepturile de acces pe care un nod le are asupra nodului conectat. Operațiile principale sunt *Take* (a lua un drept), *Grant* (a acorda un drept), *Create* (a crea un obiect sau un drept), *Remove* (a șterge un obiect sau un drept). Modelul Take-Grant implementează, prin intermediul unui digraf, maniera în care subiecții (utilizatori sau procese) pot prelua (take) și acorda (grant) drepturi altor subiecți sau obiectelor.

Pentru exemplificare, să presupunem că Alice (subiectul A) deține drepturi complete (r, w, o) asupra unui fișier F1. Bob (subiectul B) dorește să acceseze acest fișier. Alice poate folosi regula Grant pentru a acorda lui Bob drepturi de citire asupra F1. Dacă Alice are și dreptul grant "g" către Bob, atunci Bob va primi dreptul "r" asupra F1, dar nu va putea transfera acest drept mai departe dacă nu primește și dreptul de grant "g".

Modelul Take-Grant este avantajos⁷ deoarece oferă o reprezentare vizuală intuitivă, prin intermediul digrafurilor, a propagării drepturilor într-o instituție, abordând în același timp aspectul dinamic al transferului drepturilor. De asemenea, acest model permite detectarea potențialelor scurgeri de informații, și teoretic este avantajos, și des utilizat, în studiul complexității unui sistem, datorită faptului că permite o analiză formală a securității și complexității sistemului.

4. Implementările Modelului MAC

4.1. Modelul Bell-LaPadula

Din punct de vedere al securității, un sistem poate fi structurat pe niveluri de securitate, realizându-se așa-zisa securitate multinivel prin care se realizează o delimitare netă între diferite categorii de informații din sistem (publice, confidențiale, secrete, strict secrete). Modelul Bell-LaPadula, dezvoltat în 1973 de David Bell și Len LaPadula⁸, este primul model formal de securitate multinivel și, alături de modelul BIBA, rămâne unul dintre cele mai importante modele MAC. Acest model este axat exclusiv pe menținerea confidențialității informațiilor și previne scurgerea datelor către niveluri inferioare de securitate. Sensul de circulație a informațiilor, în acest model, este de sus în jos (de la nivelurile mai înalte de secretizare la cele mai joase) pentru citire, și de jos în sus (de la nivelurile mai joase la cele mai înalte) pentru scriere.

Modelul Bell-LaPadula este compus din *Subiecți* (utilizatori sau procese care încearcă să acceseze informații), *Obiecte* (resurse care conțin informații precum fișiere, baze de date), *Nivele de securitate* (clasificări ierarhice, de exemplu Public < Confidențial < Secret < Top Secret). Modelul se bazează pe două principii fundamentale:

1. *Simple Security Property* „Principiul (sau proprietatea) *Securității Simple*”, prin care nu-i este permis niciunui subiect să citească date aflate pe un nivel superior lui. Se mai

⁶ Matt Bishop, "Conspiracy and Information Flow in the Take-Grant Protection Model", in *Journal of Computer Security*, Vol. 4(4), 2000, pp. 331-360.

⁷ Reza Sadoddin, Rasool Jalili, Reza Zakeri, Ali Reza Omidian, "Network Vulnerability Analysis Through Vulnerability Take-Grant Model (VTG)", in *Proceedings of the 7th International Conference on Information and Communications Security*, 2005, pp. 256-268.

⁸ David Bell, Len LaPadula, *Secure Computer Systems, Vol. I. Mathematical Foundations, Vol. II. A Mathematical Model, Vol. III. A Refinement of the Mathematical Model*, Technical Report MTR - 2547, Mitre Corporation, March-December, 1973.

numește și principiul *No Read Up* „Nu citi deasupra”. Astfel, un subiect poate citi un obiect doar dacă nivelul de securitate (confidențialitate) al obiectului este mai mic sau egal cu nivelul de securitate al subiectului.

Pentru exemplificare, un utilizator situat pe nivelul „Confidențial” poate citi orice document clasificat pe nivelul „Public” sau pe nivelul „Confidențial”, dar nu poate citi documente clasificate ca „Secret” sau „Top Secret”.

2. *Star Property* „Principiul (sau proprietatea) *Stea*” prin care niciunui subiect nu-i este permis să scrie date într-un obiect situat pe un nivel inferior nivelului subiectului. Datorită acestui principiu, cunoscut și sub denumirea de *No Write Down* „Nu scrie dedesubt”, un subiect poate să scrie sau să modifice un obiect doar dacă nivelul de securitate al obiectului este mai mare sau egal cu nivelul de securitate al subiectului. Această regulă previne scurgerea intenționată sau accidentală a informațiilor clasificate către niveluri inferioare.

Pentru exemplificare, un utilizator situat pe nivelul „Secret” de securitate are dreptul să scrie documente situate pe nivelul „Secret” sau „Top Secret”, dar nu poate să scrie sau să modifice documente clasate „Confidențial” sau „Public” (pentru a preveni scurgerea de informații secrete).

În acest model, controlul accesului este reprezentat prin matricea din Figura 2.

Nivel Securitate	Poate Citi	Poate Scrie
Top Secret	Toate nivelurile	Doar Top Secret
Secret	Secret, Confidențial, Public	Secret, Top Secret
Confidențial	Confidențial, Public	Confidențial, Secret, Top Secret
Public	Doar Public	Toate nivelurile

Figura 2. Nivelurile de securitate și drepturile de citire și scriere pentru modelul Bell-LaPadula.

Modelului Bell-LaPadula este avantajos în primul rând datorită faptului că oferă o protecție puternică împotriva scurgerilor de informații clasificate. De asemenea, este un model relativ simplu de implementat în sisteme care necesită compartimentare strictă și teoretic reprezintă un model matematic formal care permite demonstrații de corectitudine a sistemelor de securitate. Este un model axat mai mult pe confidențialitatea datelor, nu și pe integritatea datelor. Astfel, modelul nu asigură întotdeauna integritatea datelor, de exemplu, se poate ajunge la un "write up" nedorit. Sistemul este caracterizat de rigiditate operațională, ceea ce conduce la o aplicabilitate limitată în afara mediilor militare sau guvernamentale.

4.2. Modelul BIBA

Modelul BIBA, dezvoltat în 1975 de către Ken Biba⁹, este complementar modelului Bell-LaPadula, fiind axat exclusiv pe menținerea integrității datelor, nu și pe confidențialitatea lor. Modelul BIBA previne coruperea sau modificarea neautorizată a informațiilor de către entități cu nivel inferior de credibilitate. În acest sens, în loc să clasifice informațiile după gradul de secretizare, BIBA clasifică datele și subiectele după nivelul lor de integritate sau credibilitate. Informațiile cu integritate ridicată nu trebuie să fie contaminate de informații cu integritate scăzută. Sensul de circulație a informațiilor, în acest model, este de jos în sus (de la nivelurile cu integritate scăzută la nivelurile cu integritate ridicată) pentru citire și de sus în jos (de la nivelurile înalte la cele mai joase) pentru scriere.

Ca și în cazul modelului Bell-LaPadula, există două principii fundamentale:

1. *Simple Security Property* „Principiul (sau proprietatea) *Securității Simple*”, prin care nu-i este permis niciunui subiect să citească date aflate pe un nivel inferior lui. Se mai numește și principiul *No Read Down* „Nu citi dedesubt”. Astfel, un subiect poate citi un obiect doar dacă nivelul de integritate al obiectului este mai mare sau egal cu nivelul de integritate al subiectului. Acest principiu previne ca datele cu integritate scăzută (potențial corupte) să influențeze procesele cu integritate ridicată.

Spre exemplificare, un program de gestiune financiară (integritate ridicată) nu ar trebui să citească date de la un formular web nevalidat (integritate scăzută), deoarece datele ar putea fi malițioase sau corupte.

2. *Star Property* „Principiul (sau proprietatea) *Stea*” prin care unui subiect nu-i este permis să scrie date într-un obiect situat pe un nivel superior nivelului subiectului. Datorită acestui principiu, denumit și *No Write Up* „Nu scrie deasupra”, un subiect poate să scrie sau să modifice un obiect doar dacă nivelul de integritate al obiectului este mai mic sau egal cu nivelul de securitate al subiectului. Acest principiu previne ca entități cu credibilitate scăzută să corupă date cu integritate ridicată.

Spre exemplificare, un utilizator obișnuit (integritate medie) nu ar trebui să poată modifica fișierele de configurare ale sistemului (integritate ridicată), deoarece ar putea introduce erori sau vulnerabilități.

Datorită politicilor axate în special pe Integritatea datelor, modelul BIBA are o aplicabilitate mărită și o eficiență maximă în gestionarea sistemele bancare, pentru prevenirea modificărilor frauduloase a tranzacțiilor, în gestionarea bazelor de date medicale, prin restricționarea accesului personalului autorizat la dosarele pacienților, în sistemele de control industrial, prin asigurarea protecției împotriva comenzilor malițioase, și în implementarea sistemelor ERP (planificarea resurselor întreprinderii) sau a sistemelor CRM (gestionarea relațiilor cu clienții) prin prevenirea modificării codului executabil de către procese neautorizate. Datorită faptului că, în general, multe sisteme necesită atât confidențialitate, cât și integritate mărită, se realizează o implementare hibridă dintre Bell-LaPadula și BIBA sau variante adaptate ale acestor modele.

O comparație a modelelor Bell-LaPadula și BIBA este schițată în matricea din Figura 3.

⁹ Ken Biba, *Integrity Considerations for Secure Computer Systems*, Technical Report MTR - 3153, Mitre Corporation, June, 1975.

Aspect	Bell-LaPadula	BIBA
Politică-Scop	Confidențialitate	Integritate
Regulă citire	No read up	No read down
Regulă scriere	No write down	No write up
Previne	Scurgeri de informații secrete	Coruperea datelor importante
Domeniu aplicabilitate	Militar, guvernamental	Sisteme bancare, financiare

Figura 3. Politicile și sensul de circulație a informațiilor pentru modelele Bell-LaPadula și BIBA.

5. Studiu de Caz pentru Implementarea Sistemului de Control al Accesului

În cele ce urmează vom exemplifica un studiu de caz pentru implementarea sistemului de control al accesului pentru o companie fictivă GPS SECURITY SRL de monitorizare a securității instituționale.

5.1. Contextul Organizațional

GPS SECURITY SRL este o companie fictivă de implementare și monitorizare a securității instituționale cu aproximativ 350 de angajați distribuiți în mai multe departamente: pază obiective și evenimente, monitorizare și intervenție, instalare sisteme de alarmă. Compania gestionează date extrem de sensibile, precum date financiare, rapoarte de securitate, informații despre clienți și locații, echipamente de protecție, intervenție și monitorizare. Structura organizațională este prezentată în matricea din Figura 4.

Departament	Număr Angajați	Funcții Principale
Producție	120	Asamblare aparate GPS-supraveghere
Operare	100	Administrare aparate GPS pe departamente
IT	80	Infrastructură, securitate
Contabilitate	10	Gestiune financiară, Rapoarte regulatorii, audituri
HR, Management	40	Administrare personal, direcție

Figura 4. Structura organizațională GPS SECURITY SRL.

Infrastructura IT: Compania operează o infrastructură VMware ESXi, cu 6 servere fizice care rulează mai multe mașini virtuale:

- *Firewall pfSense* – router pentru protecție perimetrală, VPN (Virtual Private Network), reguli de acces;

- *WinMentor + Oracle 19c* – sistem ERP pentru gestiune comercială și contabilitate;
- *FreeBSD + Apache* – servere web pentru aplicații interne;
- *MariaDB* – bază de date pentru loguri de la aparatele GPS;
- **BasicAirData GPS Logger** – aplicație pentru înregistrarea poziției și a traseului;
- *Active Directory (Windows Server 2022)* – autentificare centralizată, management utilizatori;
- *File Server* – stocare documentație, rapoarte, backup-uri.

Cerințele de Securitate și business ale companiei sunt:

- *Măsuri de protecție pentru conformitate* – toate accesările trebuie logate și păstrate minimum 5 ani;
- *Integritatea datelor furnizate GPS Logger* – nicio modificare neautorizată a statisticilor sau rezultatelor;
- *Separarea responsabilităților* – persoana care generează rapoartele nu poate fi aceeași cu cea care le verifică;
- *Protecția datelor financiare* – conformitate *GDPR (General Data Protection Regulation sau Regulamentul general privind protecția datelor)* pentru datele personale ale clienților;
- *Accesul rapid* pentru operatorii din teren la datele necesare;
- *Protecție împotriva fraudei interne* (angajați care încearcă să modifice statistici);
- *Accesibilitate* pentru departamentul de contabilitate la datele necesare pentru raportări;
- *Separarea clară* între datele de producție și datele operaționale.

5.2. Soluția Implementată: Model Hibrid

Pentru a răspunde cerințelor complexe, vom implementa un sistem hibrid care combină RBAC, MAC și DAC.

1. *RBAC ca bază organizațională*: Definim următoarele roluri principale, fiecare cu permisiuni specifice:

- *Admin IT* – acces complet la infrastructură, acces la date financiare ;
- *Manager Financiar* – acces citire/scriere date financiare, acces citire rapoarte de securitatea, echipament ;
- *Operator Senior* – acces citire/scriere loguri aparate, acces citire statistici locații;
- *Operator Junior* – acces doar citire pentru locația proprie;
- *Compliance Officer* – acces citire complet la toate datele fără drepturi de modificare.

2. *MAC pentru datele critice*: Implementăm principiile Bell-LaPadula și BIBA pentru protecția datelor sensibile.

Clasificarea datelor (Confidențialitate – Bell-LaPadula):

- Nivel 4 (Critic): Date financiare agregate, rapoarte și strategii de business;
- Nivel 3 (Confidențial): Loguri complete aparate, date contracte clienți/locații;
- Nivel 2 (Intern): Statistici agregate pe locații, rapoarte operaționale;
- Nivel 1 (Public): Documentație tehnică generală, proceduri standard.

Clasificarea datelor (Integritate – BIBA):

- Nivel 4 (Integritate Critică): Balanțe financiare oficiale;
- Nivel 3 (Integritate Ridicată): Rapoarte contabile, documentație oficială clienți /locații;
- Nivel 2 (Integritate Medie): Loguri operaționale, note interne;
- Nivel 1 (Integritate Scăzută): Formularele web nevalidate, input-uri utilizatori.

Reguli de acces implementate pentru Bell-LaPadula:

- Un Operator Junior (nivel 2) nu poate citi rapoarte financiare, rapoarte și strategii de business (nivel 4), loguri complete aparate, date contracte clienți/locații (nivel 3) – Principiul No Read Up;
- Un Manager Financiar sau Administrator (nivel 4) nu poate scrie în documentație publică (nivel 1) pentru a preveni scurgerea accidentală de date sensibile – No Write Down.

Reguli de acces implementate pentru BIBA:

- Procesele critice nu citesc date din surse nevalidate – No Read Down;
- Sistemele cu integritate scăzută (inputuri utilizatori) nu pot modifica balanțele financiare, rapoartele contabile, logurile operaționale – No Write Up.

3. DAC pentru flexibilitate operațională

Pentru documente și resurse care nu sunt critice, vom implementa DAC folosind ACLs (Access Control Lists) pe file server:

- Managerii pot partaja documente de lucru cu echipele lor;
- Operatorii pot crea și gestiona propriile rapoarte de teren;
- Echipa de producție poate colabora pe documentație tehnică.

5.3. Politici de Securitate Implementate

Politica de Confidențialitate:

- Toate accesările la date de nivel 3 și 4 sunt logate și revizuite săptămânal;
- Datele financiare sunt criptate în repaus (AES-256) și în tranzit (TLS 1.3);
- Accesul remote este permis doar prin VPN cu autentificare multi-factor.

Politica de Integritate:

- Datele de securitate clienți/locații sunt read-only pentru toți utilizatorii, cu excepția administratorului IT și a managerului (care pot face și modificări);
- Orice modificare în baza de date financiară necesită aprobare de la două persoane (dual control);
- Toate modificările sunt versionate și pot fi revizuite.

Politica de Disponibilitate:

- Backup-uri zilnice cu retenție de 90 zile;
- Backup-uri lunare păstrate 7 ani pentru conformitate GDPR;
- Recovery Time Objective (RTO) de 4 ore pentru sisteme critice.

5.4. Rezultate și Beneficii

Se preconizează că o implementare a sistemului de control al accesului prezentat mai sus pe o perioadă de 24 de luni ar aduce următoarele îmbunătățiri:

Securitate:

- Reducerea cu 82% a incidentelor de securitate (de la 11 incidente/an la 2 incidente/an);
- Zero încălcări ale confidențialității datelor financiare;
- Detectarea rapidă a tentativelor de fraudă internă prin sistemul de logare.

Conformitate:

- Conformitate 100% cu cerințele GDPR la audituri;
- Timp redus cu 60% pentru generarea rapoartelor de audit;
- Certificare GDPR obținută fără probleme majore.

Operațional:

- Reducerea cu 40% a timpului de on-boarding pentru angajații noi;

- Satisfacție crescută a utilizatorilor, 85% dintre angajații testați au raportat că accesul la date este simplu și rapid;
- Reducerea cu 70% a ticket-urilor de suport legate de permisiuni.

Observații finale: Considerăm că implementarea unui MAC pur pentru toate datele ar conduce la blocaje operaționale. Combinația de RBAC pentru structură, MAC pentru date critice și DAC pentru colaborare se dovedește a fi mult mai eficientă. De asemenea, se are în vedere implementarea unui dashboard care să arate în timp real tentativele de acces neautorizat, anomaliile și pattern-urile suspecte. Acest lucru permite o detectare eficientă a potențialelor probleme de securitate.

6. Concluzii

Controlul accesului în sistemele de gestiune a datelor reprezintă un element fundamental al securității informaționale moderne. În acest articol am analizat principalele modele de control al accesului – RBAC, DAC și MAC – și implementările lor specifice.

Modelul DAC, implementat prin Matricea de Control al Accesului și Modelul Take-Grant, oferă flexibilitate maximă și este potrivit pentru medii în care proprietarii de resurse necesită control discreționar. Cu toate acestea, această flexibilitate vine cu riscuri de securitate prin propagarea necontrolată a drepturilor.

Modelul MAC, materializat în implementările Bell-LaPadula (focusat pe confidențialitate) și BIBA (focusat pe integritate), oferă protecție robustă pentru date sensibile prin control centralizat și reguli stricte. Bell-LaPadula previne scurgerea informațiilor clasificate către niveluri inferioare, în timp ce BIBA protejează împotriva coruperii datelor de către entități cu credibilitate scăzută.

Studiul de caz pentru o companie fictivă GPS SECURITY SRL demonstrează că, în practică, organizațiile complexe necesită o abordare hibridă care combină elemente din mai multe modele. Implementarea noastră a combinat modelele RBAC pentru structura organizațională și simplificarea administrării, MAC pentru protecția datelor critice, și DAC pentru flexibilitate operațională în colaborare. Rezultatele obținute, anume reducerea cu 82% a incidentelor de securitate și eficiența operațională îmbunătățită, confirmă validitatea acestei abordări hibride.

În concluzie, succesul unui sistem de control al accesului nu se măsoară doar în termeni de securitate tehnică, ci și prin capacitatea sa de a permite operațiunile normale ale organizației. Un sistem prea restrictiv va fi ocolit de utilizatori, iar unul prea permisiv nu va oferi protecția necesară. Echilibrul dintre securitate și disponibilitate este cheia succesului în implementarea controlului accesului. Tendințele viitoare în controlul accesului includ utilizarea inteligenței artificiale pentru detecția anomaliilor comportamentale, adoptarea modelului Zero Trust și folosirea sistemelor de identitate managerială bazate pe cloud computing.

References

- David Bell, Len LaPadula, *Secure Computer Systems, Vol. I. Mathematical Foundations, Vol. II. A Mathematical Model, Vol. III. A Refinement of the Mathematical Model*, Technical Report MTR - 2547, Mitre Corporation, March-December, 1973.
- Ken Biba, *Integrity Considerations for Secure Computer Systems*, Technical Report MTR - 3153, Mitre Corporation, June, 1975.

- Matt Bishop, "Conspiracy and Information Flow in the Take-Grant Protection Model", in *Journal of Computer Security*, Vol. 4(4), 2000, pp. 331-360.
- Carl Landwehr, Constance Heitmeyer, John Mclean, "A Security Model for Military Message Systems", in *ACM Transactions on Computer Systems*, Vol. 2(3), August 1984, pp. 198-222.
- Andrew Lockhart, *Network Security Hacks*, O'Reilly Media Press, 2007.
- Maria Penelova, "Access Control Models", in *Cybernetics and Information Technologies*, Vol. 21(4), 2021, pp. 77-104.
- Reza Sadoddin, Rasool Jalili, Reza Zakeri, Ali Reza Omidian, "Network Vulnerability Analysis Through Vulnerability Take-Grant Model (VTG)", in *Proceedings of the 7th International Conference on Information and Communications Security*, 2005, pp. 256-268.
- Ravi Sandhu, "Role-based Access Control", in *Advances in Computers*, Vol. 46, 1998, pp. 237-286.
- Ravi Sandhu, Qamar Munawer, "How to do Discretionary Access Control Using Roles", in *Proceedings of the 3rd ACM Workshop on Role-Based Access Control*, 1998, pp. 17-54.
- Gregory Saunders, Michael Hitchens, Vijay Varadharajan, "Role-Based Access Control and the Access Control Matrix", in *Proceedings of the 5th International Conference on Information and Communications Security*, 2003, pp. 145-157.