TOP 3 SOFT-URI PENTRU SECURITATEA BAZELOR DE DATE

Valeria MUNTEANU-USCATU

Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics, group TI-201FR, Chișinau, Republic of Moldova

Autorul corespondent: Munteanu-Uscatu Valeria, valeria.munteanu@isa.utm.md

Îndrumătorul/coordonatorul științific **Dorian SARANCIUC**, lector universitar

Abstract: *Această analiză aduce în prim-plan importanța securității bazelor de date în era digitală. În contextul securității cibernetice, protejarea informațiilor sensibile stocate în bazele de date devine imperativă pentru organizații și indivizi. Abordarea noastră se concentrează asupra principalelor aspecte de securitate, inclusiv autentificarea robustă, criptarea eficientă și auditarea activităților pentru prevenirea accesului neautorizat.*

Cuvinte cheie: *securitatea bazelor de date, autentificare, criptare, auditare, responsabilitate socială.*

1. Introducere

În era digitală, în care cantitățile masive de date sunt vehiculate și stocate, securitatea bazelor de date devine un element critic pentru protejarea informațiilor sensibile și a activelor organizaționale. Din ce în ce mai multe organizații recurg la utilizarea bazelor de date pentru a gestiona eficient și stoca datele, indiferent dacă vorbim despre informații financiare, informații cu caracter personal sau alte date strategice. Odată cu creșterea dependenței de aceste tehnologii, crește și nevoia de a implementa soluții robuste de securitate pentru a contracara amenințările cibernetice din ce în ce mai sofisticate.

Securitatea bazelor de date nu este doar o preocupare tehnică, ci și o componentă esențială a managementului riscurilor în cadrul organizațiilor. Înfruntarea cu atacuri precum furtul de date, manipularea informațiilor sau distrugerea datelor devine tot mai complexă, iar reziliența la astfel de amenințări necesită adesea o combinație de tehnologii avansate, politici de securitate eficiente și educație continuă pentru personal.

În acest context, software-urile specializate în securitatea bazelor de date devin un element cheie în arsenalul de apărare cibernetică al organizațiilor. Alegerea și implementarea unor astfel de soluții reprezintă un proces strategic, având implicații directe asupra integrității, confidențialității și disponibilității datelor. În cadrul acestei analize, ne propunem să explorăm topul celor trei software-uri de referință în securitatea bazelor de date, evidențiind caracteristicile lor distinctive și contribuția adusă la întărirea perimetrelor de securitate ale organizațiilor în fața amenințărilor persistente ale lumii digitale.

2. Oracle Advanced Security

Oracle Advanced Security reprezintă o soluție avansată și specializată pentru securitatea bazelor de date Oracle, furnizând un set cuprinzător de funcționalități menite să protejeze datele sensibile și să asigure un nivel ridicat de securitate. Iată câteva aspecte relevante despre Oracle Advanced Security:

- Criptare Avansată: Unul dintre punctele forte ale Oracle Advanced Security este capacitatea sa de a oferi opțiuni extinse de criptare. Această funcționalitate asigură că datele stocate și transmise între aplicații și baza de date sunt protejate împotriva accesului neautorizat.
- Autentificare Avansată: Oracle Advanced Security include metode de autentificare avansate, contribuind astfel la protejarea identității utilizatorilor și la prevenirea

accesului neautorizat. Autentificarea robustă este esențială pentru a asigura că doar persoanele autorizate pot accesa datele sensibile.

- Securitate Transparentă: Soluția Oracle Advanced Security se integrează transparent cu mediul Oracle Database, oferind securitate fără a afecta semnificativ performanța aplicațiilor. Acest aspect este deosebit de important pentru a evita impactul negativ asupra experienței utilizatorilor și a eficienței operaționale.
- Management Avansat al Cheilor de Criptare: Oracle Advanced Security gestionează eficient cheile de criptare, permițând organizațiilor să mențină controlul asupra acestora. Administrarea centralizată a cheilor contribuie la asigurarea unei securități consistente și eficiente în cadrul întregii infrastructuri.
- Integrare cu Oracle Database: Fiind parte a ecosistemului Oracle, această soluție se integrează perfect cu Oracle Database, beneficiind de funcționalități avansate și de actualizări constante pentru a face față noilor amenințări de securitate.
- Compatibilitate cu Standardele de Securitate: Oracle Advanced Security respectă standardele de securitate, inclusiv cele referitoare la conformitatea cu reglementările privind protecția datelor (GDPR, HIPAA etc.), asigurând astfel că organizațiile pot respecta cerințele legale.

Prin aceste caracteristici, Oracle Advanced Security se impune ca o soluție de referință pentru organizațiile care doresc să își consolideze securitatea bazelor de date Oracle și să protejeze datele lor critice împotriva amenințărilor cibernetice.

3. Microsoft SQL Server Transparent Data Encryption (TDE)

Microsoft SQL Server Transparent Data Encryption (TDE) este o tehnologie integrată în platforma Microsoft SQL Server, care oferă criptare la nivel de disc pentru bazele de date. Această funcționalitate esențială contribuie semnificativ la securitatea datelor stocate în bazele de date Microsoft SQL Server. Iată câteva aspecte cheie legate de Microsoft SQL Server TDE:

- Criptare la Nivel de Disc: TDE criptează întregul set de date al unei baze de date, inclusiv fișierele de date, fișierele de jurnal și fișierele de copie de rezervă. Această criptare la nivel de disc asigură protecția datelor atât în timpul stocării, cât și în timpul transferului și copierii acestora.
- Transparență Operațională: Una dintre caracteristicile cheie ale TDE este transparența operațională. După ce este activată, TDE funcționează fără a necesita modificări semnificative ale aplicațiilor sau interacțiunii utilizatorilor. Cu alte cuvinte, procesul de criptare și decriptare are loc în mod transparent pentru aplicații și utilizatori.
- Chei de Criptare Hierarhice: TDE utilizează o ierarhie de chei pentru gestionarea procesului de criptare. Cheia de criptare a bazei de date este protejată printr-o cheie de criptare a cheilor (DEK), care poate fi ulterior protejată printr-un certificat sau o cheie asimetrică stocată în mod securizat.
- Securitate În Timpul Replicării și Copierii de Rezervă: Datorită criptării la nivel de disc, datele sunt protejate nu doar în stocare, ci și în timpul proceselor de replicare și copiere de rezervă. Astfel, TDE oferă o protecție cuprinzătoare a datelor în toate fazele ciclului de viață al informațiilor.
- Conformitate cu Reglementările: Implementarea TDE facilitează organizațiilor atingerea și menținerea conformității cu diverse reglementări și standarde de securitate, cum ar fi GDPR sau HIPAA, care impun cerințe stricte privind protecția datelor.
- Ușurința în Administrare: Microsoft SQL Server TDE este proiectat pentru a fi ușor de administrat, oferind instrumente pentru activarea, dezactivarea și gestionarea cheilor de criptare, asigurând astfel o experiență fluentă pentru administratorii de baze de date.

Prin aceste caracteristici, Microsoft SQL Server TDE devine un instrument esențial pentru organizațiile care doresc să întărească securitatea datelor lor stocate în bazele de date SQL Server, oferind o soluție robustă și eficientă în gestionarea riscurilor cibernetice.

4. IBM Guardium

Pentru IBM Guardium este o suită cuprinzătoare de soluții de securitate a datelor, proiectată pentru a oferi protecție și control avansat asupra informațiilor sensibile, în special în contextul bazelor de date. Iată mai multe detalii despre IBM Guardium:

- Auditare și Monitorizare: Una dintre funcțiile fundamentale ale IBM Guardium este să ofere facilități puternice de auditare și monitorizare a activităților în bazele de date. Prin analiza continuă a activităților, platforma identifică și raportează evenimente suspecte sau neautorizate.
- Descoperirea Datelor Sensibile: IBM Guardium este dotat cu capacități puternice de descoperire a datelor sensibile. Utilizează algoritmi avansați pentru a identifica și clasifica datele sensibile, facilitând astfel aplicarea politicilor de securitate adaptate la specificul informațiilor stocate.
- Prevenirea Pierderii de Date (DLP): Prin funcționalitățile de prevenire a pierderii de date, IBM Guardium oferă mecanisme pentru a detecta și bloca tentativele de acces sau transfer al datelor sensibile către entități neautorizate, ajutând astfel la protejarea informațiilor critice.
- Securitatea Bazată pe Politici: Platforma permite organizațiilor să implementeze politici de securitate personalizate pentru a se conforma standardelor și reglementărilor specifice industriei. Astfel, se asigură că activitățile și accesul la date sunt în concordanță cu cerințele de securitate.
- Integrare cu Baze de Date Diverse: IBM Guardium este proiectat pentru a se integra cu o gamă variată de sisteme de gestiune a bazelor de date (DBMS), inclusiv Oracle, Microsoft SQL Server, MySQL și altele. Această abordare oferă flexibilitate și acoperă o gamă largă de medii de stocare a datelor.
- Monitorizare a Accesului Utilizatorilor: Guardium oferă funcționalități avansate pentru monitorizarea accesului utilizatorilor la bazele de date. Astfel, administratorii pot detecta și investiga activitățile suspecte sau neobișnuite care ar putea indica o amenințare la adresa securității datelor.
- Gestionare a Evenimentelor de Securitate (SIEM): IBM Guardium poate integra informațiile de securitate și evenimentele într-o soluție globală de gestionare a evenimentelor de securitate (SIEM), consolidând astfel informațiile relevante într-un singur loc pentru o analiză mai eficientă și raportare.
- Monitorizare și Protecție în Timp Real: Prin monitorizarea continuă și protecția în timp real, IBM Guardium reduce riscul de pierdere de date, furnizând alerte și intervenții imediate în cazul unor activități suspecte.

IBM Guardium se adresează nevoilor organizațiilor care doresc să își întărească și să își protejeze infrastructura de baze de date în fața amenințărilor cibernetice, furnizând instrumente avansate pentru gestionarea și protejarea datelor sensibile.

Concluzii

În concluzie, securitatea bazelor de date reprezintă un aspect fundamental în era informațională, având în vedere cantitatea imensă de date sensibile stocate digital. Pentru a gestiona și proteja eficient aceste informații, utilizarea unor software-uri specializate devine o necesitate strategică. Oracle Advanced Security, Microsoft SQL Server Transparent Data Encryption (TDE) și IBM Guardium se situează în vârful clasamentului, oferind soluții avansate și cuprinzătoare pentru securitatea bazelor de date.

Oracle Advanced Security impresionează prin funcționalitățile sale avansate de criptare și autentificare, adaptându-se mediului Oracle Database pentru a oferi protecție la multiple niveluri. Microsoft SQL Server TDE furnizează o criptare transparentă la nivel de disc, asigurând securitatea datelor în toate aspectele ciclului lor de viață, de la stocare la replicare. În același

timp, IBM Guardium oferă o suită completă de soluții, de la auditare și monitorizare la prevenirea pierderii de date, cu accent pe gestionarea securității bazată pe politici.

În lumina amenințărilor cibernetice tot mai complexe, alegerea unor astfel de soluții reprezintă un pas crucial pentru organizații, asigurând integritatea, confidențialitatea și disponibilitatea datelor lor. Educația continuă, implementarea unor politici de securitate solide și adaptabilitatea la evoluțiile tehnologice reprezintă componente esențiale pentru o securitate robustă a bazelor de date într-o lume digitală în continuă schimbare. Astfel, aceste soluții nu sunt doar instrumente tehnologice, ci și piloni esențiali pentru construirea unui mediu digital sigur și încrezător.

Bibliografie

[1] *A Detailed Guide on SQL Query Optimization*. (fără an). Preluat de pe Analytics Community | Analytics Discussions | Big Data Discussion: https://www.analyticsvidhya.com/blog/2021/10/a-detailed-guide-on-sql-query-optimization/#:~:text=The%20query%20optimization%20process%20involves,plan%20based%20on%20cost%20estimations.

[2] IACOB, N. (fără an). *OPTIMIZAREA INTEROGĂRILOR*. Preluat de pe https://www.utgjiu.ro/revista/ec/pdf/2010-04.I/17_NICOLETA_IACOB.pdf

[3] *Normalizarea bazei de date*. (fără an). Preluat de pe :: Departamentul de Electrotehnica :: Facultatea de Inginerie Electrica :: Universitatea Politehnica din Bucuresti ::: http://www.elth.pub.ro/~preda/teaching/BDE/BDE_5.pdf

[4] *Query optimization*. (fără an). Preluat de pe Wikipedia: https://en.wikipedia.org/wiki/Query_optimization

[5] *The Different Types of Indexes in Databases: A Comprehensive Overview*. (fără an). Preluat de pe Medium – Where good ideas find you.: https://londondataconsulting.medium.com/the-different-types-of-indexes-in-databases-a-comprehensive-overview-559a0c4f5fb5