Аналіз засобів забезпечення додаткового захисту корпоративних баз даних

Владислав Струзік[1], Олена Харкянен[2], Сергій Грибков[3]

1. Кафедра інформаційних систем, Національний університет харчових технологій, УКРАЇНА, м. Київ, вул. Володимирська, 68, E-mail: struzik.vladislav@gmail.com

2. Кафедра інформаційних систем, Національний університет харчових технологій, УКРАЇНА, м. Київ, вул. Володимирська, 68, E-mail: helen_nuft@ukr.net

3. Кафедра інформаційних систем, Національний університет харчових технологій, УКРАЇНА, м. Київ, вул. Володимирська, 68, E-mail: sergio_nuft@ukr.net

The problems of protection of corporate databases and data warehouses are considered. The main problems that arise when multiple data are stored in data bases and data stores and secured by standard data base management systems are identified. The review and comparison of functionality and operating principles of software products was performed to improve the efficiency of protecting corporate databases and data warehouses during their operation and refactoring.

Ключові слова – захист інформації, сховища та бази даних, засоби захисту.

Вступ

Сучасне підприємство має розвинену мережеву інфраструктуру в якій працюють корпоративні інформаційні системи, що забезпечують підтримку всіх бізнес-процесів організації. Головним джерелом бізнес-інформації в такий мережевих інфраструктурах є сховища та бази даних, в них зберігається внутрішня оперативна та фінансова інформація, персональні дані співробітників, інформація про замовників та клієнтів, інтелектуальна власність, дослідження ринку та аналіз діяльності конкурентів, платіжна інформація. На сьогоднішній день, більшість фірм виробників систем управління сховищами та базами даних намагаються удосконалити засоби захисту, але їх зусилля, як правило, направлені тільки на усунення відомих вразливостей власних продуктів.

Все це призводить до необхідності забезпечення захисту не лише комунікацій, операційних систем та інших елементів інфраструктури, але й головного джерела бізнес-інформації корпоративних сховищ та баз даних. Основні методи захисту, що реалізовані у більшості СУБД, є: використання пароля; розподілення прав доступу до складових чи інформації сховища або бази даних між користувачами; шифрування й криптографія даних та програмних модулів.

Враховуючи все вище зазначене, актуальною задачею є комплексне дослідження і систематизація питань захисту сховищ та баз даних з урахуванням загальних тенденцій розвитку підходів до забезпечення інформаційної безпеки та усунення загроз.

Проблеми захисту корпоративних сховищ та баз даних

Проаналізувавши засоби забезпечення безпеки даних, реалізовані у СУБД, архітектуру сховищ та баз даних, інтерфейси систем, відомі вразливості та інциденти безпеки, було виділено основні проблеми захисту сховищ та баз даних: на належному рівні проблемами захисту інформації займаються тільки провідні фірми виробники промислових, великих СУБД; при створенні програмних продуктів розробники намагаються використовувати лише стандартні засоби захисту, що надаються СУБД; різновид масштабів та виду інформації що зберігається потребує різних підходів до безпеки; майже кожна СУБД використовує різні лінгвістичні конструкції для доступу до даних, що організовані на основі однієї моделі.

Актуальність захисту повністю пов’язана із розвитком IT-технологій, що розвиваються набагато швидше ніж інші напрямки науки та техніки. Всебічне та масове використання комп’ютерної техніки призводить до вразливості електронної інформації, що в сучасному світі стає найважливішим стратегічним ресурсом.

Основними чинниками вразливості інформації є [1]: збільшення обсягів інформації, що зберігається у сховищах та базах даних різнорідного призначення; розширення кола користувачів, що мають безпосередній доступ до ресурсів обчислювальної системи та масивів даних; ускладнення режимів роботи технічних засобів обчислювальних систем; обмін інформацією в локальних та глобальних мережах.

Основними загрозами корпоративного рівня є [1]: отримання прав доступу третьою особою; редагування, вилучення або копіювання даних без дозволу; встановлення програмного забезпечення для перехвату та передачі особистих даних та прав доступу третім особам; не дотримання елементарних правил формування та зберігання секретної інформації в одному місці або електронному документі; не використання програмних продуктів захисту при роботі з кабельними мережами; надання некоректних даних кіберзлочинцями; встановлення програм шпигунів у операційні системи; викрадення інформації, програмного забезпечення та обладнання; порушення роботи елементів системи захисту; недостатній рівень знань та недотримання правил безпеки персоналом; надання доступу до засекречених даних третім особам; фізичні пошкодження в електромережах та радіаційний влив, що призводить до втрати даних, через пошкодження носіїв інформації; стихійні лиха та непередбачені ситуації, в тому числі природні; фізичне пошкодження обладнання та елементів інфраструктури; зараження комп’ютерними вірусами та їх поширення в інфраструктурі підприємства.

Як показує практика, загрози бувають комбінованими та призводять до втрат конфіденційності та цілісності і даних, що загрожує підприємству фінансовими збитками.

Програмні продукти додаткового захисту

Авторами було проведено дослідження засобів, що представлені на сучасному ринку програмних продуктів для захисту сховищ та баз даних. Усі засоби відрізняються за призначенням, принципом дії та іншими показниками. Маємо вузько спеціалізовані продукти для шифрування даних: «BestCrypt Container Encryption», «PGPdisk», а також продукти, які являють собою системи, що організовують всебічний захист даних: «Крипто БД», «Oracle Audit Vault and Database Firewall», «McAfee Data Center Security Suite for Databases», «Елвіс Плюс», «Гарда БД».

На думку авторів доцільно виділити чотири програмні продукти, що мають, на відмінну від інших, більший спектр дії та функціонал.

«Oracle Audit Vault and Database Firewall» об'єднує ключові можливості продуктів Oracle Audit Vault і Oracle Database Firewall і при цьому розширює можливості захисту інформації для СУБД Microsoft SQL Server, SAP Sybase, IBM DB2, MySQL за рахунок підтримки аудиту каталогів операційних систем і призначених для користувача джерел даних аудиту. Він надає уніфіковану платформу моніторингу та контролю, можливості якої виходять за межі баз даних. Компоненти Database Activity Monitoring and Firewall, що входять до даного продукту, забезпечують моніторинг трафіку SQL-запитів для всіх сертифікованих версій сучасних СУБД. Методика граматичного аналізу SQL-запитів дозволяє скоротити кількість даних для аналізу, за рахунок представлення усіх запитів у вигляді кластерів, що дозволяє досягти високої точності і масштабованості, а також спростити створення списків виключень, білих і чорних списків для більш ефективного виявлення несанкціонованого доступу до баз даних, включаючи атаки типу SQL-ін'єкцій [2].

Продукт McAfee Data Center Security Suite for Databases дає фахівцям можливість отримувати повну інформацію про стан баз даних і рівні захищеності, що дозволяє повністю уніфікувати процеси управління безпекою баз даних, а також ефективно забезпечувати нормативно-правову відповідність. Комплект включає в себе продукти McAfee Database Activity Monitoring, McAfee Vulnerability Manager for Databases і McAfee Virtual Patching for Databases, що забезпечують можливість централізованого управління безпекою баз даних паралельно з іншими захисними рішеннями.

Система захисту «Елвіс Плюс» дозволяє ефективно вирішити проблему несанкціонованого доступу до інформації, що обробляється в СУБД. Базується система на програмних рішеннях Imperva SecureSphere Database Security і IBM InfoSphere Guardium, що направлені на забезпечення аудиту та захисту баз даних в реальному часі для великих корпоративних інформаційних системах. Основними функціями системи є: контроль доступу до облікових записів; оперативне виявлення та реагування на спроби несанкціонованого доступу до інформації в базі даних; можливість оперативного контролю стану захищеності баз даних.

Продукт «Гарда БД» забезпечує захист з єдиного інтерфейсу різних бізнес-додатків та СУБД. Перевагами є: функціонування в пасивному режимі з копією мережевого трафіку не впливає на роботу баз даних; здійснення контролю локальних звернень до серверу СУБД за допомогою агентського прог-рамного забезпечення; не перевищує пікове наван-таження у 5% при локальних клієнтських запитах; блокування небажаних дій користувачів баз даних здійснюється в активному режимі за рахунок мере-жевого екрану; здійснюється сканування та проведе тестування на вразливість для виявлення незаблоко-ваних облікових записи, невстановлених оновлень, облікових записів з простими паролями, активності системних облікових записів інших додатків, атак по підбору облікових записів або назв таблиць.

Розглянуті програмні продукти відрізняються за призначенням, принципом дії та іншими показниками, тому вибір необхідно роботи в залежності від завдань які він повинен вирішувати.

Висновок

Дослідження показали, що в захисті сховищ та баз даних велику роль відіграють СУБД, але не всі вони задовольняють вимогам захисту відповідного рівня. Використання додаткових засобів захисту посилять захист та завадостійкість сховищ та баз даних будь-якої організації, навіть при виконанні їх рефакторінга чи модернізації елементів корпоративних інформаційних систем.

Необхідно відмітити, що вибір додаткового засобу захисту повністю залежить від СУБД, що використовується, а також від пріоритетів та можливостей керівництва кожної фірми. Також необхідно зазначити, що використання більше ніж одного додаткового засобу захисту може призвести до виникнення конфліктів пріоритетності та перешкоджання один одному.

Література

[1] Козаченко І. П. Загальні принципи захисту інформації в банківських автоматизованих системах [Електронний ресурс] / І. П. Козаченко, В. О. Голубєв // ООО "Центр информационной безопасности". – 2005. – Режим доступу до ресурсу: http://www.bezpeka.com/ru/lib/spec/infsys/art92.html.

[2] Короткова Т. Oracle представила новый продукт для защиты баз данных [Електронний ресурс] / Т. Короткова // CNews. – 2012. – Режим доступу до ресурсу : http://www.cnews.ru/news/line/oracle_predstavila_novyj_produkt_dlya.