УДК 004.

ШИФРУВАННЯ ТА ЗАХИСТ БАЗИ ДАНИХ

Черепанська І.Ю
д.т.н., доцент, професор кафедри
комп'ютерних технологій і моделювання систем
Поліський національний університет
Складанівський Денис Валерійович
Поліський національний університет

В багатьох організаціях є власні бази даних, завдяки тому що зараз на підприємствах зберігається більше даних ніж колись, ефективна безпека стає все більш важливою. На даний момент недостатньо лише основних методів захисту безпеки, кожен раз безпеку потрібно покращувати та оновляти. Ті, хто бажає більш надійного захисту конфіденційних даних, зазвичай звертається до додаткових спеціалістів. Але мало хто на підприємствах докладає зусиль для шифрування своїх баз даних, так як це сприяє погіршенню продуктивності. Методи шифрування бази даних з часом змінились і помітно вдосконалить і в майбутньому будуть все більш вдосконалюватися. Існує декілька типів шифрування баз даних і важливо вибрати правильний тип для своєї організації, знайти баланс між складністю, посиленою безпекою та продуктивністю.

Можна сміливо сказати що захист бази даних являється актуальною проблемою і потребує вирішення.

Метою шифрування даних є захист конфіденційності цифрових даних, оскільки вони зберігаються в комп'ютерних системах і передаються за допомогою Інтернету чи інших комп'ютерних мереж. Застарілий стандарт шифрування даних (DES) був замінений сучасними алгоритмами шифрування, які відіграють важливу роль у безпеці IT-систем та комунікацій. Дані або текст шифруються за допомогою алгоритму шифрування та ключа шифрування. Результатом є зашифрований текст, який можна переглянути в оригінальному вигляді, тільки тоді коли він розшифрований правильним ключем. Шифри симетричних ключів використовують один і той же секретний ключ для шифрування та дешифрування повідомлення або файлу. Хоча шифрування симетричного ключа набагато швидше, ніж асиметричне, відправник повинен обмінятися ключем шифрування з одержувачем, перш ніж він зможе його розшифрувати. Оскільки компанії виявляють потребу в безпечному розподілі та управлінні величезною кількістю ключів, більшість служб шифрування даних адаптувались і використовують асиметричний алгоритм для обміну секретним ключем після використання симетричного алгоритму для шифрування даних.

Переваги шифрування даних:

- Це забезпечує безпеку всіх ваших даних у будь-який час
- Захищає конфіденційність та конфіденційну інформацію в будь-який час
- Захищає ваші дані на різних пристроях
- Забезпечте відповідність урядовому законодавству
- Це дає вам перевагу як конкурентна перевага
- Наявність базової технології шифрування для захисту даних може збільшити довіру
- Зашифровані дані підтримують цілісність

Можна шифрувати дані на різних рівнях, від програми до механізму баз даних. Для MSP, який розглядає, як допомогти клієнту вибрати метод шифрування, важливо чітко визначити цілі та вимоги цих різних методів шифрування:

- Метод API: це шифрування на рівні програми, яке підходить для будь-якого продукту бази даних (Oracle, MSSQL тощо). Запити в зашифрованих стовпцях змінюються в додатку, що вимагає практичної роботи. Якщо бізнес має велику кількість даних, це може зайняти багато часу. Крім того, шифрування, яке функціонує на рівні програми, може призвести до збільшення проблем із продуктивністю.
- Метод підключення: у цьому випадку ви приєднаєте модуль шифрування або пакет до системи управління базами даних. Цей метод працює незалежно від програми, вимагає менше управління та модифікації коду та є більш гнучким - ви можете застосувати це як до комерційних баз даних, так і до баз даних із відкритим кодом. За допомогою цієї опції ви зазвичай використовуєте шифрування на рівні стовпця.
- Метод TDE: прозоре шифрування даних (TDE) виконує шифрування та дешифрування в самому механізмі бази даних. Цей метод не вимагає модифікації коду бази даних або програми, і адміністраторам простіше керувати. Оскільки це особливо популярний метод шифрування баз даних, TDE детальніше розглядається нижче.

Термін прозоре шифрування даних, або "зовнішнє шифрування", означає шифрування всієї бази даних, включаючи резервні копії. Це метод, спеціально для "даних у стані спокою" в таблицях і табличних просторах, тобто неактивних даних, які в даний час не використовуються або не передаються. Все частіше прозоре шифрування даних є рідною функцією в механізмах баз даних. Це також можна обробити за допомогою шифрування накопичувача або ОС, тобто все записане на диск шифрується.

Висновки. Розробки засобів захисту даних є актуальними через збільшення обсягів цифрових даних і підсилення вимог до їх приватності та таємності. З іншого боку, розвиток технологій створює умови для незаконного дешифрування, взлому. Тому задачі шифрування даних постійно ускладнюються. Акцент слід робити на методах шифрування, серед найбільш перспективних – методи API та TDE.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Микитюк І.С., Войтович О.П. Захист баз даних шляхом фрагментування користувацького доступу // Матеріали XLVII Науково-технічноїконференціїфакультету інформаційних технологій та компютерної інженерії (2018)
2. Микитюк І.С., Баришев Ю.В. Підхід до захисту баз даних: тези на наукову конференцію//Матеріали XLVII Науковотехнічноїконференціїфакультету інформаційних технологій та компютерної інженерії (2017).
3. Полтавцева М. А., Хабаров А. Р. Безопасность баз данных: проблемы и перспективы //Программные продукты и системы. – 2016. – №. 3 (115).