Вікторія Войтко,
Алла Денисюк,
Людмила Круподьорова,
Ася Костельна

ПИТАННЯ ЗАХИСТУ СУБД ВІД МЕРЕЖЕВИХ АТАК

Стаття присвячена аналізу питання захисту СУБД від мережевих атак. Захист СУБД включає комплекс засобів, що акумулює технічні, програмно-апаратні засоби і адміністративні заходи захисту інформації. Розглянуто класифікацію атак, проведено аналіз загроз СУБД та розроблено модель системи захисту СУБД від мережевих атак.

Статья посвящена анализу вопроса защиты СУБД от сетевых атак. Защита СУБД включает комплекс средств, который аккумулирует технические, программно-аппаратные средства и административные меры защиты информации. Рассмотрена классификация атак, проведен анализ угроз СУБД и разработана модель системы защиты СУБД от сетевых атак.

Вступ

Сучасні бази даних акумулюють важливу часто конфіденційну інформацію, яка потребує ефективних систем захисту даних [1]. Тому питання захисту інформації в базах даних від несанкціонованого доступу є досить актуальним. Для його вирішення використовується комплекс засобів, що включає технічні, програмно-апаратні й адміністративні заходи, спрямовані на захист інформаційних баз [1].

Сьогодні захист конфіденційних даних постає серйозним завданням через зростання кількості та підвищення ефективності атак на інформаційні ресурси. Метою роботи є підвищення ефективності системи безпеки баз даних шляхом розробки та впровадження засобів захисту інформаційних ресурсів. Об’єктом дослідження постають процеси формування загроз СУБД. Предметом дослідження є система безпеки

СУБД. Головним завданням вбачаємо аналіз загроз СУБД та розробку моделі ефективної системи безпеки бази даних.

Аналіз питання захисту СУБД

Бази даних знаходять своє застосування практично у будь-якій галузі діяльності людини. Більшість сучасних потужних комп'ютерних програм працюють з базами даних. Очевидно, що у майбутньому бази даних будуть зберігати все більшу кількість конфіденційної інформації про персональні дані особи, її фінансові звіти, електронну медичну картку та номери кредитних карт. Заволодіння такою інформацією про особу дає зловмиснику майже необмежені можливості.

Тому захист інформації в сучасних системах управління базами даних (СУБД) є пріоритетним завданням. Викрадення конфіденційної інформації, знищення даних, викривлення інформації, виведення з ладу систем, що базуються на базах даних – далеко не повний перелік усіх ризиків, що виникають у процесі експлуатації та використання сучасних СУБД. Проте при проектуванні системи захисту бази даних завжди існує проблема економічної доцільності, тобто вартість системи захисту не має перевищувати вартість ресурсів, які оберігаються.

Захист бази даних є однією з простих задач захисту інформації. Це обумовлено тим, що бази даних мають чітко визначену внутрішню структуру, і операції над елементами баз даних також чітко визначені. Зазвичай над елементами баз даних визначено лише чотири основні операції: пошук, введення даних, заміна і видалення інформації. Інші операції носять допоміжний характер і використовуються відносно рідко [2]. Тож проста структура системи захисту спрощує її адміністрування і сильно ускладнює завдання подолання захисту СУБД.

Аналіз загроз СУБД

У більшості випадках зловмисники навіть не намагаються атакувати СУБД, оскільки подолати захист автоматизованої системи на рівнях операційної системи та мережі набагато простіше. Тим не менш, в окремих

випадках подолання зловмисником захисту конкретної СУБД є цілком можливим. Такі ситуації трапляються, якщо [3]:

• в автоматизованій системі використовується СУБД, захист якої недостатньо надійний;

• використовується недостатньо добре протестована версія СУБД, що містить помилки в програмному коді;

• адміністратори бази даних допускають грубі помилки при визначенні політики безпеки.

Відомі дві небезпечні атаки СУБД, для захисту від яких потрібно використовувати спеціальні заходи [1]:

• "атака салямі", коли значення округлення результатів арифметичних операцій додається до значення деякого елемента бази даних (наприклад, до суми, що зберігається на особистому рахунку зловмисника);

• статистична ідентифікація – атака, що дозволяє отримувати конкретні значення тих полів бази даних, для яких доступна тільки статистична інформація; основна ідея атаки полягає в такому визначенні параметрів запиту, щоб безліч записів, за якими збирається статистика, включали в себе тільки один запис.

Розглянемо кілька поширених способів отримання інформації про обліковий запис для доступу до бази даних. Перший спосіб – це простий перебір можливих паролів, коли атакуюча сторона намагається використовувати найпоширеніші комбінації паролів до облікових записів адміністратора бази даних в надії знайти можливі співпадіння. Інший спосіб отримання пароля базується на недбалості самих користувачів, коли задля власної зручності адміністратори залишають паролі до облікових записів у місцях, куди мають доступ треті особи, наприклад, на власному робочому місці. Це дозволяє зловмиснику викрасти облікові дані, не прикладаючи до цього великих зусиль.

Сучасні виробники встановлюють пароль для привілейованого облікового запису за замовчуванням або залишають його порожнім. SQL Server поставляється з привілейованим обліковим записом "SA" та порожнім паролем. Даний обліковий запис за замовчуванням відключений, але при інсталяції MS SQL Server існує можливість його підключення і встановлення власного паролю. Часто адміністратори лише встановлюють власний пароль, не змінюючи при цьому назви облікового запису. Це значно спрощує процедуру підбору пароля, адже в Інтернеті існують тисячі списків з комбінаціями паролів. Наявність привілейованих облікових записів, таких як "SA", зі слабким механізмом аутентифікації надає можливість легкого атакування СУБД та отримання доступ до неї.

Розробка системи захисту СУБД

Розроблена система захисту СУБД спрямована на протидію атакам, орієнтованим на реалізацію методу повного перебору можливих варіантів логіну і паролю, та атакам, що здійснюють підбір пароля до стандартних облікових записів, таких як “SA” або “sysdba”. Модель запропонованої системи захисту СУБД від мережевих атак наведена на рис. 1.

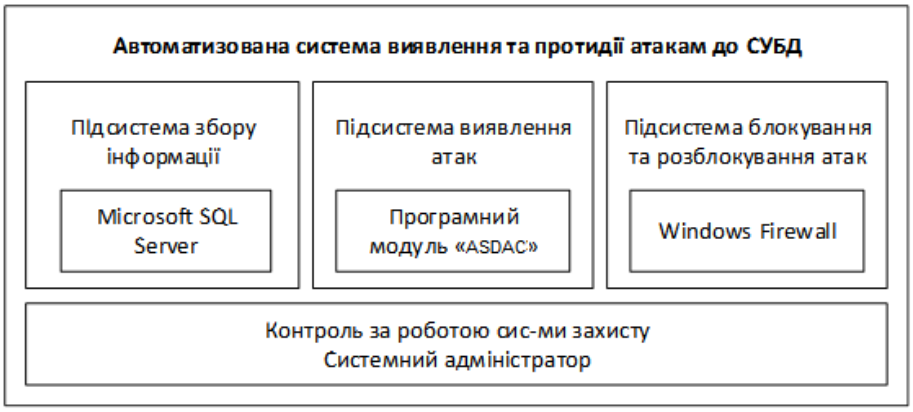

Рисунок 1 – Модель системи захисту СУБД

Запропонована модель системи захисту СУБД має модульну структуру, що дозволяє виявляти й ідентифікувати атаки і протидіяти їм на різних рівнях системи захисту даних. Підсистема блокування атак являє собою модуль-надбудову до мережевого екрану Windows.

Даний модуль в режимі реального часу відслідковує зміни в списку заблокованих IP-адрес та вносить відповідні зміни до брандмауера

Windows. Для автоматизації процесу встановлення правил інформаційного захисту даних використовується бібліотека interop.netfwtypelib.dll, яка дозволяє створювати, модифікувати та видаляти правила зі списку правил вбудованого брандмауера FireWall. Розроблена система захисту СУБД орієнтована на роботу в автоматизованому режимі. Крім того, програмно забезпечена можливість ручного керування адміністратором процесу блокування IP-адрес та створення власних правил захисту системи.

Висновки

Наявні загрози СУБД включають можливості мережевих атак на інформаційні ресурси баз даних. Питання розробки ефективних і економічно обґрунтованих засобів захисту СУБД потребує системного підходу до вибору методів та шляхів реалізації політики безпеки системи управління базою даних.

Запропонована система захисту СУБД від мережевих атак орієнтована на протидію атакам, спрямованим на підбір паролів доступу до інформаційних ресурсів та облікових записів. Розроблена система захисту оснащена графічним інтерфейсом, що забезпечує автоматизований і ручний режими визначення правил захисту даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Тарасов Д.О. Специфічні для СУБД загрози захисту інформації // Защита информации: Сб. науч. тр. – К.: НАУ, 2001. – С. 53-60.

2. Тарасов Д.О. Обмежений набір операцій для роботи з базами даних / Д.О.Тарасов, А.М.Пелещицин, П.І.Жежнич // Вісн. Нац. ун-ту “Львівська політехніка”. – 2001. – № 438. – С. 125–131.

3. Bonatti P.A, Foundations of Secure Deductive Databases / P.A. Bonatti, S.Kraus, V.S. Subrahmanian, // IEEE Transactions on Knowledge and Data Engineering. – 2011. – Vol. 7, No. 3. – P. 406–422.