ОСНОВНІ АСПЕКТИ БЕЗПЕКИ БАЗ ДАНИХ

Єрастова В. Ю., студ. (гр. КП-81мн, ФПМ КПІ ім. Ігоря Сікорського);
Праховнік Н. А., к.т.н., доц. (каф. ОППЦБ КПІ ім. Ігоря Сікорського)

Анотація: Питання захисту даних є критичними при забезпеченні безпеки сучасних корпоративних систем. Тези присвячені ситуації, що склалася в області безпеки даних, що знаходяться під управлінням систем БД.

Ключові слова: база даних, інформаційна безпека, уразливість, захист даних, безпека даних.

Abstract: Data protection issues are critical when ensuring modern enterprise systems security. The paper is devoted to the current situation in database systems security.

Keywords: database, information security, vulnerability, data protection, data security.

Внутрішня операційна інформація компанії, персональні дані співробітників, фінансова інформація, інформація про замовників і клієнтів, інтелектуальна власність, дослідження ринку, аналіз діяльності конкурентів, платіжна інформації – це відомості, які найчастіше цікавлять кіберзлочинців, і майже завжди вони зберігаються в корпоративних базах даних.

Значимість і цінність цієї інформації призводить до необхідності забезпечення захисту не тільки елементів інфраструктури, а й самих баз даних. Спробуємо комплексно розглянути і систематизувати питання безпеки різних систем управління базами даних (СУБД) в світлі нових загроз та загальних тенденцій розвитку інформаційної безпеки.

Майже всі великі виробники СУБД обмежуються розвитком концепції конфіденційності, цілісності і доступності даних, а їхні дії спрямовані, в основному, на подолання існуючих і вже відомих уразливостей, реалізацію основних моделей доступу і розгляд питань, специфічних для конкретної СУБД. Такий підхід забезпечує вирішення конкретних завдань, але не сприяє появі загальної концепції безпеки для такого класу ПЗ, як СУБД. Це значно ускладнює завдання по забезпеченню безпеки сховищ даних на підприємстві.

Історично розвиток систем безпеки баз даних відбувався як реакція на дії зловмисників.

Можна виділити наступні архітектурні підходи [2]:

– повний доступ всіх користувачів до сервера БД;
– поділ користувачів на довірених і частково довірених засобами СУБД;
– введення системи аудиту (логів дій користувачів) засобами СУБД;
– введення шифрування даних; винесення засобів аутентифікації за межі СУБД в операційні системи і проміжне ПЗ; відмова від повністю довіреного адміністратора даних.

Введення засобів захисту як реакції на загрози не забезпечує захист від нових способів атак і формує розрізнене уявлення про саму проблему забезпечення безпеки.

З урахуванням таких еволюційних особливостей з’явилась і існує велика кількість різнорідних засобів забезпечення безпеки, що в підсумку призвело до відсутності розуміння комплексної безпеки даних. Відсутній загальний підхід до безпеки сховищ даних. Ускладнюється і прогнозування майбутніх атак, а також розробка захисних механізмів.

Проаналізувавши засоби забезпечення безпеки СУБД, архітектуру БД, відомі уразливості і інциденти безпеки, можна виділити наступні причини виникнення такої ситуації [3]:

– проблемами безпеки серйозно займаються тільки великі виробники;

– інженери баз даних, прикладні програмісти і адміністратори не приділяють належної уваги питанням безпеки;

– різні масштаби і види збережених даних вимагають різних підходів до безпеки;

– різні СУБД використовують різні мовні конструкції для доступу до даних, організованих на основі однієї і тієї ж моделі;

– з’являються нові види і моделі зберігання даних.

Сховища даних включають в себе два компоненти: збережені дані (власне БД) і програми управління (СУБД).

Забезпечення безпеки інформації, що зберігається, зокрема, неможливо без забезпечення безпечного управління даними. Виходячи з цього, всі уразливості і питання безпеки СУБД можна розділити на дві категорії: залежні від даних і не залежать від даних. Уразливості, що не залежать від даних, є характерними і для всіх інших видів ПЗ. Їх причиною, наприклад, може стати несвоєчасне оновлення ПЗ, наявність не використовуваних функцій або недостатня кваліфікація адміністраторів ПЗ.

Більшість аспектів безпеки СУБД є саме залежними від даних. У той же час багато уразливостей є побічно залежними від даних. Наприклад, більшість СУБД підтримують запити до даних з використанням деякої мови запитів, що містить набори доступних користувачеві функцій або довільні функції на мові програмування. Архітектура вживаних мов безпосередньо пов’язана з моделлю даних, яка застосовується для зберігання інформації. Таким чином, модель визначає особливості мови, і наявність в ній тих чи інших уразливостей. Причому такі уразливості, наприклад, як ін'єкція, виконуються по-різному (sql-ін’єкція, java-ін’єкція) в залежності від синтаксису мови [4].

Для вирішення зазначених проблем забезпечення інформаційної безпеки СУБД необхідно перейти від методу закриття уразливостей до комплексного підходу забезпечення безпеки сховищ інформації. Основними етапами цього переходу, повинні стати наступні положення:

– розробка комплексних методик забезпечення безпеки сховищ даних на підприємстві.

– оцінка і класифікація загроз і уразливостей СУБД.

– розробка стандартних механізмів забезпечення безпеки.

Література

1. Информационная безопасность бизнеса. Исследование текущих тенденций в области информационной безопасности бизнеса. 2014. URL: http://media.kaspersky.com/pdf/IT_risk_ report_Russia_2014.pdf.

2. Lesov P. Database security: a historical perspectiv. 2010. URL: http://arxiv.org/ftp/arxiv/papers/1004/1004.4022.pdf.

3. Top Ten Database Security Threats. URL: http://www.imperva.com/docs/wp_topten_database_threats.pdf .

4. Murray M.C. Database security: what students need to know. JITE:IIP, vol. 9, 2010, pp. 61–77.