Полотай Орест Іванович,
к.т.н., ст. викладач
Львівський державний університет безпеки життєдіяльності, Львів

АНАЛІЗ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ СИСТЕМ КЕРУВАННЯ БАЗАМИ ДАНИХ

Згідно з проведеними дослідженнями про розслідування витоків даних, у більш ніж 92 % випадків витоку даних відбуваються з систем управління базами даних (СКБД). Причиною цього є те, що в більшості компаній недостатній рівень захисту СКБД.

В зв'язку з цим, у роботі проведено дослідження програмного забезпечення, яке забезпечує надійний захист інформації, що зберігається в СКБД. **Актуальність дослідження** полягає в тому, що в умовах сьогодення стрімко збільшуються можливостей зловмисників, щодо викрадення інформації, що в свою чергу, пов'язано із стрімким розвитком ІТ-технологій.

Серед відомих програмних комплексів, які надають можливість надійно захищати інформацію, яка ними обробляється, варто виділити програмний комплекс McAfee [1].

Програмний комплекс забезпечує надійний захист і безперервну нормативно-правову відповідність без необхідності вносити зміни в архітектуру, купувати дороге апаратне забезпечення і час від часу відключати бази даних.

У програмний комплекс McAfee для захисту баз даних включено ряд кращих у своєму роді продуктів, що забезпечують комплексний захист, який значно перевершує за можливостями вбудовані в СКБД функції безпеки, що легко піддаються атакам зловмисників. Завдяки модульному характеру рішень McAfee для захисту баз даних існує можливість індивідуального налаштування засобів захисту з метою автоматизації процесів управління виявленням, захистом, моніторингом та безпекою баз даних.

Для того, щоб забезпечити надійний захист СУБД від внутрішніх та зовнішніх загроз, програмне забезпечення, яке для цих цілей планується використовувати, повинно відповідати наступним вимогам:

моніторинг активності і змін: реакція програмного забезпечення на будь-які відхилення від встановлених правил безпеки;

засоби аудиту для найбільш достовірного звіту подій, повинні працювати в автономному режимі, щоби навіть адміністратор системи не зміг їх відключити (виключення людського фактору);

запобігання простоїв, викликаних установкою виправлень: комплекс повинен виявляти атаки з використанням відомих вразливостей, а також визначати шляхи поширення загроз;

сумісність з «хмарними» системами: використання віртуальних центрів обробки даних і «хмарних» обчислень для ефективного аналізу мережевого трафіку з метою виявлення порушень політик.

Для задоволення вище поставлених вимог, програмний комплекс McAfee пропонує два продукти, спеціально розроблених для забезпечення захисту СКБД -

McAfee Vulnerability Manager for Database та McAfee Database Activity Monitoring (рис. 1).

Програмний продукт McAfee Vulnerability Manager for Databases проводить понад 3000 перевірок на наявність вразливостей в базах даних всіх поширених типів, включаючи Microsoft SQL Server, IBM DB2 і MySQL.

Програмний продукт McAfee Database Activity Monitoring, використовуючи більше 380 встановлених правил, дає змогу здійснювати візуальний контроль і запобігати вторгнення в реальному часі з метою блокування порушення до нанесення збитку.

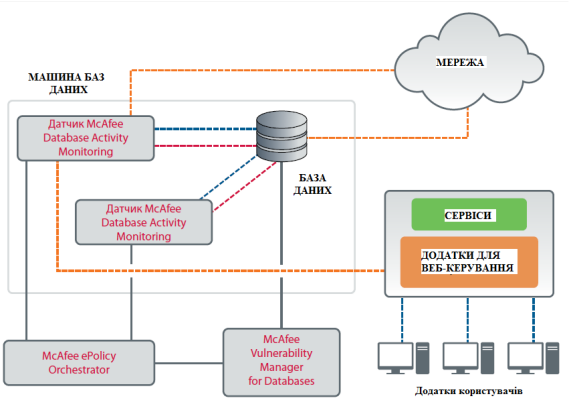

Рис. 1. Схема роботи програмних продуктів McAfee

Отже, програмний комплекс McAfee для захисту СКБД забезпечує захист критично важливих для усіх видів діяльності баз даних в режимі реального часу від усіх видів загроз.

Список використаних джерел

2. Офіційний сайт компанії Intel Security-McAfee [Електронний ресурс]. – Режим доступу з http://www.McAfee.com

Фетісов Валерій Сергійович,
к.ек.н., доцент
Ніжинський державний університет ім. М. Гоголя, м. Ніжин

ФОРМУВАННЯ ОБМЕЖЕННЯ ДОСТУПУ ДО ДАНИХ КОРИСТУВАЧІВ В КОНФІГУРАТОРІ ПЛАТФОРМИ 1С:

Останнім кроком створення прикладного рішення є формування обмежень доступу до даних користувачів. Адміністрування списку користувачів та надання їм прав відповідно до службових обов'язків є дуже важливим моментом для організації інтерфейсу прикладного рішення у цілому та розмежування дій окремих користувачів.

Обмеження прав доступу користувачів реалізується комбінацією таких методів:

– призначенням ролі кожному користувачеві;