УДК 004.6

БЕЗПЕКА БІЗНЕС-СИСТЕМ ТА БАЗ ДАНИХ В КОНТЕКСТІ АНАЛІЗУ МЕТОДІВ І ЗАСОБІВ КІБЕРБЕЗПЕКИ

Привалов М.І., здобувач вищої освіти, acc.muptup@gmail.com,
Національний університет «Одеська політехніка»
Ніколаєв Д.П., асистент кафедри економіки, nikolaevdmytro0504@gmail.com,
Національний університет «Одеська політехніка»

Відомо, що бізнес-система являє собою категорію процесної моделі організації, що виражена за допомогою системного підходу в організації в рамках процесного управління [1]. У свою чергу, система управління базами даних (СУБД) - це комплекс програмно-мовних засобів, які воліють створити бази даних (БД) і управляти даними. Іншими словами, СУБД - це набір програм, що дозволяє організовувати, контролювати і адмініструвати бази даних [1]. Все далі сказане застосовується як до СУБД, так і до бізнес-систем.

Дані - це цінний об'єкт (інформаційний актив) організації, з яким необхідно надійно поводитися і керувати ним, як і з будь-яким ресурсом. Таким чином, деяка частина або всі комерційні дані можуть мати тактичне значення для організацій і, відповідно, повинні бути захищені і конфіденційні.

Безпека БД відноситься до набору інструментів, елементів управління і заходів, призначених для встановлення і збереження конфіденційності, цілісності і доступності БД, як еталонної моделі (тріади) інформаційної безпеки (ІБ) [1]. Але в контексті даної статті хочеться приділити основну увагу конфіденційності, оскільки саме цей елемент піддається ризику в більшості випадків витоку і компрометації даних.

Безпека БД повинна враховувати і захищати наступне:

- самі дані в БД і СУБД;
- будь-які зв'язні програми та програми;
- фізичні та віртуальні сервери БД;
- обчислювальна та мережева інфраструктура для доступу до БД.

Безпека БД - складне завдання, що включає всі аспекти технологій і методів забезпечення ІБ. При цьому страждає один з принципів забезпечення ІБ - доступність [2]:

- чим доступніше і зручніше БД, тим більше вона вразлива для загроз без небезпеки інформації (УБІ);
- чим більш невразлива БД для УБІ, тим важче отримати до неї доступ і використовувати її.

Необхідність забезпечення безпеки БД.

Застосування належних методів забезпечення безпеки БД важливо для будь-якої організації з цілого ряду причин. Це включає:

1. Забезпечення безперервності бізнесу.

2. Мінімізація фінансових збитків.

3. Втрата інтелектуальної власності.

4. Збиток репутації бренду.

5. Покарання і штрафи.

Загрози безпеці інформації в БД.

Перелічимо ряд найбільш відомих причин і типів кіберзагроз без небезпеки БД:

1. Внутрішні загрози. Це БД з одного з наступних трьох джерел, кожен з яких має привілейовані засоби доступу до БД [3]:

- інсайдер зі злим умислом;

- недбалий співробітник, який піддає БД атаці необережними діями;

- сторонній, який отримує облікові дані за допомогою соціальної інженерії або інших методів.

Особлива увага - внутрішні користувачі (особливо ключові з працівниками), які часто не визнаються актуальними порушниками. Таким чином, внутрішня загроза є однією з найбільш типових причин порушення безпеки БД і часто виникає через те, що багатьом співробітникам надано доступ привілейованого користувача теля.

2. Людський фактор [3].

3. Експлуатація вразливостей ПЗ [2].

4. Атаки з ін'єкціями SQL/NoSQL. Будь-яка СУБД вразлива для цих атак, якщо розробники не дотримуються методів безпечного програмування [3].

5. Атаки на переповнення буфера. Зловмисники можуть використовувати надлишкові дані, що зберігаються в сусідніх адресах пам'яті, як відправної точки для запуску атак [3].

6. Атаки типу «відмова в обслуговуванні» (DoS/DDoS). При розподіленій атаці типу «відмова в обслуговуванні» (DDoS) підроблений трафік генерується великою кількістю комп'ютерів, що беруть участь в ботнеті, що тролюється зловмисником [2]. Це створює дуже великі обсяги трафіку, які важко зупинити без добре масштабованої захисної архітектури [3].

7. Шкідливе ПЗ. Захист від шкідливих програм важлива для будь-якій кінцевій точці, але особливо для серверів БД через їх високу цінність і чутливість

8. IT-середовище, що розвивається. IT-середовище, що розвивається, робить БД більш сприйнятливими до загроз. Тенденції, які можуть призвести до але вим типів атак на БД або можуть зажадати нових захисних заходів:

- зростаючі обсяги даних;

- розподілена інфраструктура;

- посилюються нормативні;

- брак навичок в області забезпечення кібербезпеки.

Методи забезпечення безпеки БД

Як було сказано раніше, для забезпечення хорошої безпеки нам потрібно врахувати безліч нюансів. Оскільки БД майже завжди доступні з мережі, будь-яка БД для будь-якого компонента або частини мережевої інфраструктури також є загрозою, і будь-яка атака, що зачіпає пристрій або робочу станцію користувача, може загрожувати БД. Таким чином, безпека БД повинна виходити далеко за межі однієї тільки БД.

При оцінці безпеки БД необхідно розглянути кожну з областей [2]:

1. Фізична безпека.
2. Адміністративне та мережеве управління доступом.
3. Безпека облікового запису/пристрою кінцевого користувача.
4. Шифрування.
5. Безпека та актуальність ПЗ БД.
6. Безпека програми/веб-сервера.
7. Безпека резервного копіювання.
8. Аудит ПЗ БД, системного та прикладного ПЗ.

Висновок. Відповідно, пошук слідів компрометації інфраструктури необхідно проводити комплексно, беручи до уваги максимально широке коло джерел виявлення БД. Крім того, необхідно регулярно проводити оцінку зрілості процесів ІБ організації, включаючи методи тестування на проникнення - PenTest, для отримання реального стану рівня захищеності інфраструктури. Це якісно спрощує розслідування інцидентів і реагування на них.

У висновку слід зазначити, що підхід до забезпечення безпеки бізнес-систем і СУБД з можливістю інтеграції розглянутих вище методик стане ефективніше не тільки в стадії експлуатації, але і на етапі створення систем захисту інформації і буде більш практико-орієнтованим. Це поліпшить здатність протистояти УБІ, активно виявить поведінку зловмисників і підтримувати надійний, контекстуально двонаправлений обмін інформацією.

Список використаних джерел

1. Бізнес-система (Глосарій процесного управління)//Технології BPM і ERP від Пітер Софт URL: https://piter soft.ru/knowledge/glossary/process/bizines-sistema.html (дата звернення: 27.02.2024).
2. Захист баз даних//Науково-технічний центр ЄВРААС URL: https://www.evraas.ru/solutions/db-protection/(дата звернення: 28.02.2024).
3. Казарян К.К. Безпека бази даних//Науково-освітній журнал для студентів та викладачів. КНЕУ, Економіка. Київ, Генеза, № 1 - 2022.