Проведені дослідження на виявлення нейромережею перших чотирьох атак показало, що вони можуть успішно справлятися з визначенням цих атак з великою точністю. Для виявлення п'ятого і шостого типів атак застосовувалися рекурентні нейронні мережі, які орієнтовані на обробку послідовних значень.

Таким чином, можна з упевненістю стверджувати, що дослідження в області захисту даних користувачів з використанням нейронних мереж відкрили перспективні можливості для використання їх у сфері кібербезпеки.

Список використаних джерел:

1. Нейромережа STAMINA. URL: https://www.iguides.ru/main/security/microsoft_i_intel_sozdayut_idealnyy_antivirus/.
2. Штучний інтелектURL: https://spydell.livejournal.com/633585.html.
3. Нейромережі в кібербезпеки. URL: https://habr.com/ru/post/587694/

Науковий керівник: доцент Задерейко О.В.

МЕТОДИ ЗАХИСТУ БАЗ ДАНИХ

Маскименко А.С.

студентка 1 курсу факультету адвокатури та антикорупційної діяльності Національного університету «Одеська юридична академія»

Сучасні компанії обов’язково мають свою особисту конфіденційну інформацію різних видів, яку треба забезпечити максимальну безпеку в середовищі бази даних.

База даних (БД) – це впорядкований набір логічно взаємопов’язаних даних або сукупність матеріалів, які можуть бути найдені і оброблені за допомогою комп’ютера. БД використовується спільно, та призначена для задоволення інформаційних потреб користувачів.

Система керування базами даних (СКБД) - це комплекс програмних і мовних засобів, необхідних для створення баз даних, підтримання їх в актуальному стані та організації пошуку в них необхідної інформації.

Головним завданням БД є збереження значних обсягів інформації (даних).

На сьогоднішній день існують такі аспекти захисту інформації [1]:

- цілісність;
- захист інформації від несанкціонованої модифікації;
- конфіденційність;
- захист від несанкціонованого ознайомлення з інформацією;
- доступність в сенсі підтримання системи в робочому стані та способи швидко відновити втрачену чи пошкоджену інформацію.

Відповідно, до даних аспектів захисту інформації, виділяють такі загрози:

- загрози цілісності (знищення та модифікація інформації);

- загрози доступності (блокування та знищення інформації);
- загрози конфіденційності (несанкціонований доступ, витік та розголошення інформації).

Безпека баз даних – це комплекс організаційно-технічних заходів і правових норм для попередження заподіяння збитку інтересам власника інформації (в тому числі від незаконного використання та шкідливих загроз та атак).

Методи захисту баз даних в СКБД

Захист надійним паролем [2]. Надійність пароля є мірою ефективності від його вгадування або брутфорс атак. У своїй звичайній формі, він оцінює, скільки спроб зловмисникові, не маючи прямого доступу до пароля, потрібно, в середньому, щоб правильно вгадати його. Сила пароля – це функція, що враховує довжину, складність і непередбачуваність. Захист паролем – є самим простим способом захисту БД від несанкціонованого доступу. Паролі можуть бути встановленні користувачами або адміністраторами. Їх облік і зберігання виконується СКБД. Паролі зберігаються в спеціальних файлах СКБД в зашифрованому вигляді. Після введення пароля користувачу надається доступ до необхідної інформації. Не дивлячись на простоту парольного захисту, він має ряд недоліків. По-перше, пароль є вразливим, особливо якщо він не шифрується при зберіганні в СКБД. По-друге, користувачу потрібно запам'ятати або записати пароль, а при недбалому відношенні до запису пароль може стати надбанням інших.

Наявність резервних копій. Ефективним способом для запобігання втраті інформації може бути фіксація всіх копій і БД. Під час виконання резервного копіювання інформації для врахування всіх критично важливих даних треба провести попередню інвентаризацію. Не всі дані є критично важливими або потребують захисту, тому на них немає сенсу витрачати час і ресурси.

Шифрування [3]. Після ідентифікації критично важливих даних потрібно застосувати надійні алгоритми шифрування конфіденційної інформації. Кращий спосіб захистити базу даних – зашифрувати зробити прочитання неможливим для осіб, що не володіють ключами шифрування. Важливою особливістю будь-якого алгоритму шифрування є використання ключа, який стверджує вибір якогось конкретного методу кодування із всіх можливих. Розрізняють два основні методи шифрування: симетричне й асиметричне. В симетричному шифруванні один і той же ключ використовується і для шифрування, і для дешифрування. В асиметричних методах застосовуються два ключі. Один з них, несекретний, використовується для шифрування і може публікуватися разом з адресою користувача, другий, секретний, застосовується для дешифрування і відомий тільки одержувачу. Шифрування забезпечує всі три аспекти безпеки даних: конфіденційність, цілісність і доступність.

Розділення прав доступу до об'єктів БД. Треба організовувати обмеження дозволів та привілеїв. Власник об'єкта, а також адміністратор БД мають всі права. Решта користувачів мають ті права і рівні доступу до об'єктів, якими їх наділили. Дозвіл на доступ до конкретних об'єктів бази даних зберігається в файлі робочої

групи. Файл робочої групи містить дані про користувачів групи і зчитується під час запуску. Файл зберігає наступну інформацію: імена облікових записів користувачів, паролі користувачів, імена груп, в які входять користувачі.

Для розділення прав доступу до об'єктів БД слід застосувати:

- обмеження доступу до конфіденційних даних для певних користувачів і процедур, які можуть робити запити, пов'язані з конфіденційною інформацією;
- обмеження використання основних процедур тільки певними користувачами;
- уникнення використання і доступу до баз даних у не робочий час.

Захист полів і записів таблиць БД. Так як у комп'ютерній базі даних вся інформація подається у таблиці, то захист полів і контенту таблиць є ключовим аспектом захисту інформації.

Забезпечення цілісності зв'язків таблиць. Всі таблиці БД мають кореляційні зв'язки, тому будь-яке мінімальне несанкціоноване втручання може мати великі негативні наслідки.

Базу даних слід розміщувати на сервері, недоступному безпосередньо через мережу Інтернет, щоб запобігти віддаленому доступу зловмисників до корпоративної інформації. Важливе значення також має фізична безпека сервера баз даних та резервного обладнання від крадіжок та стихійних лих.

Безпечне використання застосунків. Деякі застосунки містять вразливості, що піддаються атакам. Вразливості та ризики, пов'язані з конфіденційністю, можуть використовуватися зловмисниками для отримання несанкціонованого доступу до інформаційних ресурсів організації або даних користувача. Вразливі застосунки ініціюють з'єднання з мережею, іншими застосунками або сторонніми сервісами, що робить необачного користувача більш вразливим до атаки зловмисників.

Оновлення системи та зміна налаштувань за замовчуванням. Рекомендується також вимкнути всі служби і процедури, які не використовуються.

Вбудовані засоби контролю даних. Вони є доступними але не завжди можуть повністю вирішити виникаючі на практиці проблеми. Спеціалізовані програмні засоби захисту інформації від несанкціонованого доступу володіють в цілому кращими можливостями і характеристиками, ніж вбудовані засоби.

Організація спільного використання об'єктів БД в мережі. Сьогодні проблема доступу користувачів до віддалених баз даних, може вирішуватися за допомогою створення та використання локальних і глобальних мереж передачі даних, а також надання відповідного доступу до баз даних користувачам. База даних може бути локальною, коли користувач підключається до неї безпосередньо, і віддаленою - у випадку підключення до неї на великій відстані. Підключення до віддаленої бази даних здійснюється за допомогою мережевого забезпечення та відповідних протоколів передачі даних. Слід зазначити, що

використання Web-технології для доступу до БД має забезпечити надійний захист інформаційних потоків. Це досягається створенням брандмауерів - апаратно-програмних систем міжмережевого захисту від несанкціонованого доступу до сервера БД.

Процедури ідентифікації, автентифікації і авторизації в СКБД [4]. Сутність процедури ідентифікації полягає в призначенні користувачу БД – імені. Ім'я користувача – це деяка унікальна мітка, що відповідає прийнятим угодам і забезпечує однозначну ідентифікацію об'єкта реального світу в просторі об'єктів, що відображаються. Сутність процедури автентифікації полягає в підтвердженні автентичності користувача, що представив ідентифікатор. У ряді сучасних СКБД використовується:

- біометрична автентифікація - це процес доведення і перевірки автентичності заявленого користувачем імені через пред'явлення користувачем своїх біометричних характеристик (наприклад, відбитки пальців і долоні, звуки голосу, обличчя, відбиток сітківки ока, особливості роботи на клавіатурі, електронний цифровий підпис);
- парольна автентифікація - це процес доведення і перевірки автентичності заявленого користувачем імені шляхом введення ним пароля або парольної фрази. Парольні фрази забезпечують більшу безпеку, ніж короткі паролі, але вимагають більшого часу для введення. Заходами, що дають змогу підвищити надійність парольного захисту є: накладання технічних обмежень, управління терміном дії паролів, обмеження доступу до файлу паролів, обмеження кількості невдалих спроб входу в систему, використання програмних генераторів паролів;
- автентифікація із застосуванням токенів. Токен - це предмет або пристрій, володіння яким підтверджує автентичність користувача.

Переведення непродуктивних баз даних в анонімні [5]. Багато компаній інвестують час та ресурси у захист своїх продуктивних баз даних, але при розробці проекту або створення тестового середовища вони просто роблять копію вихідної бази даних і починають використовувати її в середовищах з менш жорстким контролем, тим самим розкриваючи всю конфіденційну інформацію. За допомогою маскування та анонімізації можна створити аналогічну версію з тією ж структурою, що і оригінал, але із зміненими конфіденційними даними для їх захисту. За допомогою цієї технології значення змінюються за умови збереження формату. Дані можуть бути змінені шляхом змішування, шифрування, переставляння символів або заміни слів. Конкретний метод, правила і формати, залежать від вибору адміністратора, але незалежно від вибору, метод повинен забезпечити неможливість отримати вихідні дані за допомогою зворотної інженерії. Цей метод рекомендовано використовувати для баз даних, які є частиною середовища тестування і розробки, оскільки він дозволяє зберегти логічну структуру даних, забезпечуючи відсутність доступу до конфіденційної інформації поза виробничим середовищем.

Проведення моніторингу активності БД. Аудит і відстеження дій всередині бази даних передбачає знання про те, яка інформація була оброблена, коли, як і ким. Володіння повною історією транзакцій дозволяє зрозуміти шаблони доступу до даних і модифікацій і, таким чином, допомагає уникати витоку інформації, контролювати небезпечні зміни і виявляти підозрілу активність в режимі реального часу.

Перегляд існуючої системи на предмет будь-яких відомих або невідомих уразливостей та визначення та реалізація дорожньої карти/плану їх зменшення.

Можна зробити висновок що використання лише якогось певного методу не може гарантувати повного зберігання даних. Тому для підвищення рівня безпеки інформації в БД рекомендовано використання комплексних заходів.

Розробки в сфері безпеки БД є дуже актуальними та потребують майже не щоденного вдосконалення.

Особливої актуальності ця проблема набула в час російсько-української війни, коли задля безпеки на рівні держави вжили максимальних заходів - закрили повний доступ для всіх державних реєстрів, тим самим відсікли їх від глобальної мережі.

Список використаних джерел:

1. Касянчук, Н. В., Ткачук Л. М. Захист інформації в базах даних. URL: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/download/7001/5715. 2019
2. Як створити надійний пароль — рекомендації спеціалістів ESET. URL: https://eset.ua/ua/news/view/649/nadezhnyy-parol-sposoby-sozdaniya-parolya- ot-spetsialistov-eset
3. Шифрування та захист баз даних. URL: https://iitd.com.ua/shifruvannj a-ta-zahist-baz-danih/
4. Системи управління базами даних. URL: http: //rodak.if. ua/komptech/lection4 .htm
5. Защита баз данных – залог безопасности корпоративной сети. URL: https: //eset.ua/ua/blog/view/14/

Науковий керівник: доцент Задерейко О.В.

ЗАСОБИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У МЕРЕЖІ ІНТЕРНЕТ

Максимчук А.Ю.

студентка 1 курсу судово-адміністративного факультету факультету Національного університету «Одеська юридична академія»

Сьогодні інтернет всюди проник у наше життя і діяльність. Користувачі використовують його кожен день, починаючи з соціальних мереж і до онлайн-банкінгу. Також цей ресурс який використовується для навчання і праці.