ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

Осельський Сергій Віталійович

Методика захисту конфіденційності інформації в базах даних mssql і mysql від sql-атак

Спеціальність 125 «Кібербезпека»

Автореферат

дипломної роботи на здобуття освітньо-кваліфікаційного рівня «магістр»

Тернопіль — 2019

Дипломною роботою є рукопис.

Роботу виконано у Тернопільському національному технічному університеті імені Івана Пулюя.

Керівник роботи: кандидат технічних наук, доцент
Козак Руслан Орестович
Тернопільський національний технічний університет імені Івана Пулюя,

Рецензент: кандидат фізико-математичних наук, професор, завідувач кафедри ММ
Михайлишин Михайло Стахович
Тернопільський національний технічний університет імені Івана Пулюя

Захист відбудеться __ грудня 2019 р. о __ год. на засіданні Державної екзаменаційної комісії у Тернопільському національному технічному університеті імені Івана Пулюя за адресою:
46001, м. Тернопіль, вул. Танцорова, 2.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність дослідження. Станом на 2019 рік діяльності організацій все більше залежать від комп'ютерних технологій, так і проблеми захисту інформації стають все більш актуальними. Кожен збій в системі роботи баз даних призводить до відчутних матеріальних втрат.

Мета і завдання дослідження. Метою дипломної роботи є розгляд та створення методики захисту баз даних mySQL та MSSQL

Реалізація мети дослідження обумовленна такими реалізаціями:

1. Проаналізувати статистику атак на різні галузі, такі як: виробництво, бакнківську, школи.
2. Дослідити вразливості бази даних mySQL та MSSQL
3. Дослідити методи та найкращі практики захисту інформації в базах даних
4. На основі рішень та вимог сформувати методику захисту інформаціїї

Об'єктом дослідження дипломної роботи є ефективна і безперебійна робота баз даних.

Предметом дослідження є створення методики захисту баз даних від будь-яких кібератак.

Методи дослідження. В даній роботі використанно методи порівняння, дедукції, системного підходу, аналізу і синтезу.

Нормативно-правовою базою дослідження є Закон України "Про захист інформації в інформаційно-телекомунікаційних системах". Інформаційною основою дипломної роботи є праці вітчизняних та зарубіжних вчених з питань визначення ефективності безпеки роботи баз даних.

Наукова новизна роботи. Полягає у тому, що вперше створена методика на основі синтезу найефективніших та доступних рішень на різних рівнях захисту інформації в базах даних.

Практичне застосування дослідження полягає застосуванні декількох технологій захисту баз даних на всіх етапах роботи, а саме:

1. Метод плейхолдерів для борьби з sql-ін'єкціями
2. Метод TOTP для безпеки автентифікації

3. Метод Blockchain для захист від будь-яких фальсифікацій даних.

Апробація результатів дослідження. Основні положення та результати дослідження обговорювалися та були схвалені на VII Науково-технічній конференції “Інформаційні моделі, системи та технології” (Тернопіль, 2019).

Структура роботи. Робота складається із анотації, вступу, 6-ти розділів, висновків, списку використаних джерел обсяго 71 найменувань. Робота містить 20 рисунків та 13 лістингів. Обсяг основного тексу становить 92 сторінки, перелік використаних джерел - 7 сторінок. Загальний обсяг дипломної роботи складає 120 сторінок.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність проблеми, визначено об’єкт і предмет дослідження, сформульовано його мету, завдання, розкрито теоретичну та методологічну основу, методи дослідження; висвітлено наукову новизну, практичне значення роботи; подані відомості про апробацію результатів дослідження.

У Першому розділі - - проаналізовані підходи до трактування поняття ефективності діяльності підприємств, проведено дослідження атак та їх типів на різні галузі діяльностей

Визначено поняття «ефективність» як ступінь досягнення цілей при мінімальному споживанні ресурсів для їх досягнення на всіх етапах та складових процесу із врахуванням балансу задоволення інтересів зацікавлених сторін як критерію для вірного окреслення цілей.

Аналізуючи дану статистику, можна визначити типи атак, для яких баз даних підприємств доволі вразливі. За даною теорією можна скласти певний план для реалізації захисту, захистившись від найбільш актуальних проблем.

У II кварталі 2019 року кібер-зловмисники націлені на експлуатацію:CVE-2017-11882; CVE-2019-0708; CVE-2019-0604; CVE-2019-

2725; CVE-2019-10149; CVE-2019-3396. Хакери активно експлуатують вразливість у поштовому сервері Exim (CVE-2019-10149), яка дозволяє віддалено виконувати команди операційної системи (ОС) з правами адміністратора. Одне з хакерських угруповань використовує цю вразливість для впровадження бекдор, завантажуючи на поштові сервери shell-скрипти і додаючи SSH-ключ до облікового запису root.

Крім того, зловмисники незаконно завантажують на вразливі сервери ПЗ для майнингу криптовалюті. Вразливість була усунена розробниками Exim у лютому 2019 року. Однак випуск поновлення ПЗ виробником не завжди нейтралізує загрозу, і через несвоєчасне оновлення ПЗ хакери успішно експлуатують вразливості навіть п'ятирічної давності.

Найбільш обговорення набула проблема безпеки у II кварталі з критично небезпечною RCE-вразливістю BlueKeep (CVE-2019-0708) у використанні RDS деяких старих версій Windows. Незважаючи на те, що 14 травня 2019 року компанія Microsoft випустила патч, більшість комп'ютерів по всьому світу залишаються під загрозою, в той час як зловмисники продовжують активно шукати вразливі вузли і розробляти експлойти.

Отже, основними принципами захисту інформації є її конфіденційність, цілісність і достовірність. Захист інформації потребує централізованості, плановості, конкретики і цілеспрямованості, активності, надійності і універсальності, а також мати економічний ефект. Захист інформації існує на рівні робочого місця користувача, на рівні підрозділу і всього підприємства. Є чотири групи захисту інформації: технічні, програмні, змішані і організаційні. Найбільш вразливою є інформація в інтернеті, а тому рекомендується використовувати надійні паролі, шифрування даних,

антивірусні програми, а також налаштовувати паролі на BIOS для її ефективного захисту.

Кіберзагрози –- це сукупність факторів і умов, що створюють небезпеку порушення інформаційної безпеки. Цілеспрямовані атаки переважають над масовими і становлять 59% усіх атак. Більшість з них спрямована на викрадення інформації у фізичних чи юридичних осіб для отримання фінансової вигоди. Серед найпоширеніших загроз інформаційній безпеці варто відзначити використання шкідливого ПЗ, соціальну інженерію, хакінг, експлуатації веб-вразливостей, підбір облікових даних.

У другому розділі- - розглянуто метод використання плейхолдерів, як основу для захисту від sql-інєкцій.

SQL ін'єкція – це техніка введеня коду, яка використовується для атаки неправильно написані запити і вставляють інші значення для досягнення своїх цілей.

Більшість статей, присвячених ін’єкціям пропускають цей момент. Але реальність така, необхідно підставляти не тільки дані в запити, але й інші елементи, такі як ідентифікатори, елементи синтаксису, ключові слова. Навіть такі незначні елементи як DESC чи AND, але потреба в безпеці таких підстав все рівно повинні бути не менш строгими.

Розберемо звичайний випадок. В нас є база товарів, яку необхідно вивести на екран користувачу в вигляді HTML таблиці. Особа яка використовує дану таблицю, може проводити будь-які дії відносно даних в таблиці, що приводить до значень які може використовувати користувач, а саме: атрибути та ідентифікатори. Використання даних значення на пряму в запит – це гарантована ін’єкція. Методи форматування до яких усі привикли

тут не допоможуть. Підготовка вираження ні з яким ідентифікатором, ні з ключовим словом не приведуть до потрібного результату. Єдине правильне рішення в цій ситуації – це білий список.Це звичайне поняття і практично всі досвідченні розробники легко добавляють його у потрібні запити.

Для використання даного методу, нам необхідно щоб усі дані були прописані в коді в якості змінних, що унеможливлює ін'єкцію в даний запит.

Суть даного методу у тому, що всі можливі варіанти вибору повинні бути чітко прописані в нашому коді, і в запит попадатимуть тільки вони, на основі користувацького вводу.

У третьому розділі - - проаналізовано два методити захисту, метод авторизації за допомогою TOTP та захисту розподілених баз даних Blockchain.

На сьогоднішній день все більше компаній використовують одноразові паролі для збільшення рівню безпеки клієнтів та їх персональних даних. Ці компанії в основному використовують алгоритм HOTP - який створює хешованне значення використовуючи певні параметри, за рахунок чого досягається безпека. Але все більшої популярності отримує алгоритм TOTP - який використовує алгоритм HOTP з однією особливістю - він базується на часі.

Авторизація за допомогою алгоритму TOTP і HOTP є ефективними сучасними методами захисту конфіденційної інформації в базах даних. Їх основою є хеш-функція, яка дозволяє взяти дані будь-якої довжини і побудувати «цифровий відбиток пальця» за цими даними. Безпека алгоритмів TOTP і HOTP є засобами запобіганню двом найпоширенішим атакам: атака виду "людина посередині" і атака повторного відтворення. Їх функція

полягає у застосуванні лічильника, який періодично змінює дані, які використовують для генерації одноразових паролів.

Блокчейн організовує зростаючий перелік записів транзакцій в ієрархічно розширюваному ланцюгу блоків, захищеним методами криптографії, щоб забезпечити міцну цілісність своїх записів транзакцій. Нові блоки можуть бути задіяні у глобальну блок-ланцюзі лише після їх успішної конкуренції з децентралізованою процедурою взаємозгоди. Окрім інформації про записи транзакцій, блок також тримає у собі хеш-значення всього блоку, що може розглядатися як його криптографічне зображення, плюс хеш-значення попереднього блоку, який слугує криптографічним зв'язком з попереднім блок в блокчейн. Децентралізована процедура взаємозгоди застосовується мережею, яка контролює прийом нових блоків до ланцюга блоків, протокол зчитування для безпечної перевірки ланцюга блоків та узгодженість вмісту даних записів транзакцій, що містяться у кожній копії блокчейна та підтримуються на кожному вузлі. Як результат, блокчейн забезпечує те, що запис транзакцій буде доданий до блоку, а блок, у свою чергу, буде успішно створений та зафіксований у блокчейні.

Запис транзакцій не може бути змінено або порушено у ретроспективі. Цілісність вмісту даних у кожному блоці ланцюга гарантовано таким чином, що блоки, потрапивши в блокчейн, не можуть бути замінені жодним чином. У результаті, блок-ланцюг служить захистом для розподіленої книги, яка ефективно перевіряє усі операції між двома сторонами відкритої мережевої системи.

У контексті біткойн-систем блокчейн використовується як його захищений, приватний та надійний публічний архів для всіх транзакцій, які торгують біткойнами в мережі. Це гарантує, що всі транзакції з біткойнами

записуються, організовуються та зберігаються в криптографічно захищених блоках, які є ланцюжками у певній та стійкій формі.

Blockchain – це головний захист біткойн-транзакцій від багатьох поширених атак. З розвитком технології blockchain, Bitcoin вплинув на його застосування в інших галузях, таких як охорона здоров'я, логістика, сертифікація освіти. Екосистема блокчейна стрімко зростає зі збільшенням інвестицій та інтересів промисловості, уряду та наукових установ у введенні децентралізованих систем баз даних.

Три основні можливості, які підтримуються реалізацією блокчейна в Bitcoin:

1. Хеш-накопичувальне сховище (Hash Chained Storage).
2. Цифровий підпис.
3. Зобов'язання щодо додавання нового блоку до глобально ланцюгового сховища.

З правильним поєднанням набору відомих методів безпеки, таких як ланцюг Hash, дерево Merkle, цифровий підпис, з механізмами взаємозгоди, блокчейн може запобігти як проблемі подвійного витрачання біткойнів, так і не дозволити зміну будь-яких даних транзакцій в блоці іншою датою.

Блокчейн стійкий до несанкціонованих дій. Користувачам дозволено повертатися до певного блоку та перевіряти його з початку ланцюга. Дерево Merkle є двійковим деревом пошуку з вузлами, пов'язаними між собою за допомогою хеш-показників. Така структура даних використовується для побудови блокчейна.

ВИСНОВКИ

Отже, основними принципами захисту інформації є її конфіденційність, цілісність і достовірність. Захист інформації потребує централізованості,

плановості, конкретики і цілеспрямованості, активності, надійності і універсальності, а також мати економічний ефект. Захист інформації існує на рівні робочого місця користувача, на рівні підрозділу і всього підприємства. Є чотири групи захисту інформації: технічні, програмні, змішані і організаційні. Найбільш вразливою є інформація в інтернеті, а тому рекомендується використовувати надійні паролі, шифрування даних, антивірусні програми, а також налаштовувати паролі на BIOS для її ефективного захисту.

Кіберзагрози –- це сукупність факторів і умов, що створюють небезпеку порушення інформаційної безпеки. Цілеспрямовані атаки переважають над масовими і становлять 59% усіх атак. Більшість з них спрямована на викрадення інформації у фізичних чи юридичних осіб для отримання фінансової вигоди. Серед найпоширеніших загроз інформаційній безпеці варто відзначити використання шкідливого ПЗ, соціальну інженерію, хакінг, експлуатації веб-вразливостей, підбір облікових даних.

Узагальнюючи всю роботу ми отримуємо методику взаємодій декількох сучасних способів захисту баз даних. Використовуючи кожен з методів ми отримуємо універсальну формулу захисту від будь-як актуальних типів атак на бази-даних.

Анотація

Осельський С. Методика захисту конфіденційності інформації в базах даних MS SQL та mySQL від sql-атак

У роботі досліджено методи захисту інформації на рівні баз даних та авторизації. Проаналізовано основні принципи і методи захисту інформації. Запропоновано методи захисту баз даних від стороннього втручання. Розроблено метод захисту конфіденційності інформації в базах даних MS SQL.

Ключові слова: SQL-ін’єкції, MS SQL, mySQL, конфіденційність, авторизації, блокчейн.

Abstract

Oselskyi S. Methods of information confidentiality protection in mssql and mysql data bases

The methods of data protection in databases at the level of databases and authorization are investigated. The basic methods of information protection are analyzed. Methods for protecting databases from third-party interference are suggested. A method of protecting the privacy of information in MS SQL databases has been developed.

Key words: SQL-injection, MS SQL, mySQL, privacy, authorization, blockchain.