Ключові слова: DDoS-атаки, DNS-сервера, IP-адресу, запобігання, відстеження**,** законодавчі аспекти.

Ключевые слова: DDoS-атаки, DNS-сервера, IP-адрес, предотвращение, отслеживание, законодательные аспекты.

Keywords: DDoS-attacks, DNS-servers, IP-address, prevention, tracking, legislative aspects.

Науковий керівник: *к.т.н., доц. Задерейко О.В.*

Іванова Ірина Олександрівна

Національний університет «Одеська юридична академія»,

студентка 3-го курсу факультету кібербезпеки та інформаційних технологій

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ БАЗ ДАНИХ

Актуальність теми обумовлена зростанням використання інформаційних баз у державних установах, корпораціях та підприємствах. Вторгнення, викрадення або пошкодження яких призводить до руйнівних наслідків у фінансовій, репутаційній, а інколи й в юридичній сферах.

Можна виокремити декілька основних причин які привертають увагу до безпеки даних та змушують використовувати більше ресурсів задля забезпечення безпеки БД.

Насамперед це кіберзлочинність, засоби якої постійно удосконалюються, з’являються нові способи проникнення до систем, створюється нове шкідливе програмне забезпечення та віруси.

По-друге, це проблема юридичної відповідальності. Права людини в міжнародному законодавстві про захист персональних даних являються одним з основоположних в інформаційному просторі, а отже постійно змінюються і стають все більш суворими. Відповідальність за недотримання нормативних

вимог, щодо збереження конфіденційних даних покладається на організації, котрі отримують її в ході діяльності.

Процес захисту систем баз даних охоплює сукупність програмних засобів, процесів та технологій, використання яких запобігає несанкціонований доступ, модифікацію, порушення цілісності, знищення або копіювання [1].

Захист будь-якої інформаційної системи, в такому випадку БД має бути багаторівневим, а отже діяти комплексно. Система безпеки не повинна обмежуватись лише базою даних, адже при доступі через мережу, будь-яка вразливість компоненту мережної інфраструктури, робочої станції або пристрою користувача буде являтись загрозою для інформаційної системи. Високорівнева система захисту повинна складатись з:

- Безпеки на фізичному рівні. Незалежно від розміщення бази даних(на локальному сервері або в хмарному сховищі) це має бути захищене місце, з контролем фізичного доступу до обладнання.
- Адміністративного контроль надання прав доступу. Користувачам повинні надаватись мінімальні права доступу, згідно з задачами які вони виконують.
- Безпеки пристроїв та облікових запитів. Забезпечення моніторингу доступу до БД та дій з даними. Контроль даних дозволяє вчасно отримувати інформацію про нетипові або підозрілі маніпуляції з даними. Кожний пристрій який під’єднано до мережі інформаційної системи, має бути захищений фізично.
- Шифрування та токенізації (технологія, що дозволяє забезпечити електронні платежі за допомогою системи шифрування даних). Дані в БД та ідентифікаційні дані користувачів, повинні бути захищені в процесі передачі та під час зберігання шляхом шифрування. Для захисту особливо конфіденційних даних бажано використовувати токенізацію.
- Безпеки програмного забезпечення. Необхідно вчасно встановлювати останні версії ПЗ, оскільки при кожному оновленні знешкоджується цілий ряд помилок та потенційних загроз.

- Безпеки веб-серверу. Необхідно забезпечити безперервне тестування безпеки серверу, який взаємодіє з БД, адже він може стати каналом проведення атаки.
- Безпеки резервних копій. Кожна копія або образ БД мають бути захищені на такому ж рівні, як і сама інформаційна система.
- Аудиту. Реєстрація кожної виконаної дії або зміни на сервері, в операційній системі та базі даних. Проведення регулярного аудиту щодо забезпечення кібербезпеки [2].

Окрім, формування багаторівневої системи захисту в мережі, необхідно організувати контроль та безпечний доступ до бази даних, шляхом впровадження: адміністративного контролю (керування змінами та конфігураціями БД), профілактичний контроль (управління доступом та шифруванням), виявлення (запобігання несанкціонованого доступу до інформаційної системи).

Політики інформаційної безпеки, які регулюють інформаційну діяльність в організації задля цілісного забезпечення та підтримки інформаційної безпеки БД, повинні бути успадковані хмарним середовищем. Крім того, мають бути визначенні відповідальні особи за обслуговування та аудит заходів безпеки. Формальні політики безпеки повинні бути підкріплені програмним навчанням, підвищенням обізнаності користувачів у сфері кібербезпеки, визначенням стратегій тестування на можливість проникнення та оцінка вразливостей системи [3].

Список використаних джерел:

1. Machine Learning and Security: Protecting Systems with Data and Algorithms / C. Chio, F. David., 2018. 386 с.

2. Database Security Best Practices: The Essential Guide 2021. URL: https://securityintelligence.com/articles/database-security-best-practices-essential-guide/

3. Consumer Privacy and Data Protection / Daniel J. Solove, Paul M. Schwartz., 2020. 422 с.

Ключові слова: база даних, інформаційна система, безпека.

Ключевые слова: база данных, информационная система, безопасность.

Keywords: data base, information system, security.

Науковий керівник: *к.т.н., доц. Кухаренко С.В.*

Кравченко Іван Сергійович

Національний університет «Одеська юридична академія»,

студент 3 курсу факультету кібербезпеки та інформаційних технологій

МЕТОДИ ЗАХИСТУ ВІД DDOS-АТАК

Мета атаки DDoS (Distributed Denial of Service) – домогтися відмови в обслуговуванні пристроїв які спроможні з’єднуватись з Інтернетом: обладнання мережевого контролю, різних Інтернет-магазинів, веб-сайтів та веб-додатків, інфраструктури Інтернету речей. Найбільша кількість атак у мережі розгортаються наступними кроками:

1) збір даних про цільовий об’єкт та їх аналіз з метою виявлення найбільш видимих та уразливих недоліків системи, вибір способу атаки;

2) націлюватися до атак шляхом підготовки зловмисного коду на комп'ютерах і всіх підключених до мережі Інтернет пристроях, які були перехоплені та встановлені під контроль зловмисника;

3) створення багаточисельних запитів з більшості підконтрольних пристроїв;

4) підведення підсумків атаки.

Якщо бажаний результат не був виконаний, в багатьох випадках буде проведений повторний та більш якісний аналіз, і знову повторення першого кроку.

При умовах успішної атаки на WEB-додаток, або базу даних, цільовий