Секція 1

ДОСЛІДЖЕННЯ ТА РОЗРОБКА МОДЕЛІ ЗАГРОЗ КОМЕРЦІЙНОГО ВЕБ-СЕРВІСУ

Кислицин О. О.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Пєвнєв В. Я.

Актуальність. Не можна заперечувати, що онлайн-шопінг популярний у наш час. Дослідження показують, що це більше, ніж просто тенденція. Клієнти продовжуватимуть звертатися до Інтернету щоразу, коли хочуть зробити роздрібну покупку. Згідно дослідженням Forbes Adviser очікується, що світовий ринок електронної комерції у 2023 році становитиме 6,3 трильйона доларів, та що до 2026 року ринок електронної комерції становитиме понад 8,1 трильйона доларів [1]. У той же час найуразливішою галуззю є електронна комерція, яка зазнає 32,4% атак у різних формах [2].

За останні кілька років у галузі електронної комерції сталася низка витоків даних. Ці порушення не тільки збільшують репутаційні, фінансові та операційні ризики, але й вічно переслідують бізнес електронної комерції, оскільки одне порушення даних коштує компанії в середньому 3,86 мільйона доларів і займає 280 днів для локалізації [3]. 10,5 трильйонів доларів. Саме стільки коштуватиме компаніям кіберзлочинність до 2025 року – за даними Cyber Ventures, це 15% ріст кожного року [4]. Тому актуальність кібербезпеки для поточних та нових комерційного веб-сервісу як ніколи висока.

Метою даної роботи є дослідження безпеки та розробка моделі загроз яка буде слугуватиме структурованим фреймворком, який ідентифікує, аналізує та класифікує потенційні загрози та вразливості, характерні для комерційних веб-сервісів.

Основні положення. Для розробки моделі загрози доступні кілька систем і методологій. Деякі широко використовувані фреймворки безпеки веб-служб включають: модель STRIDE – забезпечує структурований підхід до ідентифікації загроз з точки зору цих категорій, допомагаючи систематично оцінювати ризики; модель DREAD – це система оцінки ризиків, яка використовується для кількісного визначення серйозності виявлених загроз і визначення пріоритетів на основі їх потенційного впливу; методологія OCTAVE зосереджена на виявленні та оцінці ризиків з точки зору бізнес-цілей, інформаційних активів і вразливостей, надаючи цілісне уявлення про ризики безпеці; методологія PASTA – це методологія, орієнтована на ризик, яка об’єднує моделювання загроз, оцінку ризиків і симуляцію атак для систематичного аналізу загроз і визначення відповідних заходів безпеки.

Використовуючи ці фреймворки та методології, організації можуть прийняти структурований підхід до моделювання загроз і підвищити ефективність своїх заходів безпеки.

Висновки. У сучасному цифровому ландшафті комерційні веб-сервіси відіграють вирішальну роль у сприянні онлайн-транзакцій, комунікації та обміну інформацією. Однак із зростанням довіри до веб-сервісів зростає й потреба вирішувати постійну загрозу, яка створює значні ризики для їх безпеки. Щоб забезпечити захист цінних даних, важливо розробити ефективні моделі загроз, спеціально адаптовані до унікальних проблем, з якими стикаються комерційні веб-сервіси. Моделювання загроз має першочергове значення в сфері безпеки веб-служб. Воно забезпечує структурований підхід до виявлення та оцінки потенційних загроз, характерних для комерційних веб-служб, що дозволяє організаціям покращити розуміння ризиків безпеки та дати можливість постачальникам веб-послуг запровадити надійні заходи безпеки для захисту своїх систем, даних клієнтів і загальних бізнес-операцій.

Список літератури

1. 38 E-Commerce Statistics Of 2023. *Forbes Advisor*. URL – https://www.forbes.com/advisor/business/ecommerce-statistics (дата звернення: 08.02.2023);
2. E-Commerce Security Infographics – Statistic, Issues, And Solutions for 2022. *LinkenIn Nitesh Behani blog*. URL – https://www.linkedin.com/pulse/e-commercesecurity-infographics-statistic-issues-nitesh-behani- (дата звернення: 17.05.2022);
3. Major e-commerce data breaches: What we can learn from them. *DataQuest magazine*. URL – https://www.dqindia.com/major-e-commerce-data-breaches-whatwe-can-learn-from-them (дата звернення: 10.08.2022);
4. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. *Cybercrime magazine*. URL – https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025 (дата звернення: 13.11.2020).

Відомості про авторів

Кислицин Олександр Олександрович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.o.kyslytsyn@student.csn.khai.edu

Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., доцент, v.pevnev@csn.khai.edu