Секція 1

ВИКОРИСТАННЯ МЕТОДОЛОГІЇ OSINT ДЛЯ ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ ФІНАНСОВИХ СТРУКТУР

Проценко Д. І.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Пєвнєв В. Я.

Актуальність. Кількість кібератак у світі постійно збільшується, одним з головних об'єктів для кіберзлочинців є фінансовий сектор. Це пов'язано з тим, що фінансові організації володіють великою кількістю конфіденційної інформації та значними фінансовими ресурсами, що становлять велику цінність. Застосування методів OSINT (Розвідка з відкритих джерел) допомагає суттєво знизити ризики атак, виявляючи потенційні загрози на ранніх етапах [1].

Метою роботи є аналіз використання методології OSINT для підвищення рівня кібербезпеки фінансових структур, визначення її ролі у виявленні та нейтралізації кіберзагроз, а також розробка рекомендацій щодо ефективної інтеграції OSINT у систему безпеки фінансових установ.

Основні положення. Методологія OSINT базується на використанні загальнодоступної інформації, такої як новини, дані з соціальних мереж, форуми тощо. Основною метою OSINT – аналіз та виявлення корисної інформації для кіберрозвідки, моніторингу загроз, аналізу кібератак тощо. Одними з найбільш популярних інструментів є: Maltego – платформу для аналізу даних у реальному часі, яка допомагає виявити приховані зв'язки; Shodan – для моніторингу підключених до інтернету пристроїв і відкритих портів; DarkOwl – для сканування DarkWeb на предмет витоків або підготовки атак [2].

Використання OSINT у фінансовому секторі може суттєво підвищити ефективність виявлення та запобігання кіберзагрозам, за допомогою моніторингу широкого спектру джерел, включаючи DarkWeb. Якісними прикладами роботи OSINT є: виявлення скомпрометованих облікових даних, моніторинг активності хакерських груп, ідентифікація фішингових сайтів. Виявлення таких загроз на ранньому етапі знижує ризик подальших атак, захищаючи клієнтів та репутацію компанії [3].

Незважаючи на це все, потрібно пам'ятати, що необхідно враховувати етичні та правові аспекти, пов'язані з конфіденційністю та захистом персональних даних. Наприклад, збір персональних даних без дозволу,

навіть якщо вони доступні у соцмережах, може порушувати законодавство про захист даних [4].

Висновки. OSINT є важливим компонентом сучасної системи кібербезпеки, що дозволяє фінансовим установам оперативно реагувати на загрози та мінімізувати ризики. Використання такого інструменту рекомендоване для створення повноцінного комплексу систем захисту інформації.

Список літератури

1. Rising Cyber Threats Pose Serious Concerns for Financial Stability. *International Monetary Fund*. URL – https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability (дата звернення 14.11.2024).
2. The Beginner's Guide to Open-Source Intelligence (OSINT): Techniques and Tools. *Medium*. URL – https://medium.com/@techmindxperts/the-beginners-guide-to-open-source-intelligence-osint-techniques-and-tools-6a91b9c37ee1 (дата звернення 14.11.2024).
3. How Open Source Intelligence Can Protect You From Data Leaks. *Builtin*. URL – https://builtin.com/articles/osint-protect-data-leaks (дата звернення 14.11.2024).
4. Legal and ethical considerations in OSINT investigations. *HackerAcademy*. URL – https://hackeracademy.org/legal-and-ethical-considerations-in-osint-investigations (дата звернення: 14 листопад 2024).

Відомості про авторів

Проценко Данило Ігорович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.i.protsenko@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