УДК 004.056
К. Николин
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗВІДКА ВІДКРИТИХ ДЖЕРЕЛ ІНФОРМАЦІЇ ДЛЯ ВИЯВЛЕННЯ ЗАГРОЗ БЕЗПЕКИ БІЗНЕСУ

K. Nykolyn

OPEN SOURCE INTELLIGENCE FOR IDENTIFYING BUSINESS SECURITY THREATS

Світові підприємства працюють в епоху цифрової трансформації. Це дає безліч переваг для компаній: допомагає покращити клієнтський досвід, продуктивність й управління ресурсами. Але разом із цими перевагами, більш широке впровадження технологій також означає збільшення можливості компрометації даних.

Open-source intelligence (OSINT) – розвідка на основі аналізу відкритих джерел інформації) – одна з форм процесу організації та управління збором розвідувальних даних (Intelligence Collection Management), що включає їх пошук і відбір із публічних загальнодоступних джерел, добування та аналіз інформації, формування розвідувального документу для прийняття відповідного рішення [1]. Процес OSINT складається зі збору, обробки, аналізу даних та формування звіту після їх виявлення. У світі кібербезпеки OSINT найчастіше використовується на ранніх стадіях тестування на проникнення, при цьому ця інформація також доступна і суб'єктам загроз; етап розвідки забезпечує базу для пошуку вразливостей для експлуатації з технічної точки зору. Кожна організація має модифіковану структуру OSINT відповідно до своєї мети, оскільки вимоги до OSINT відрізняються від однієї організації до іншої. Проте OSINT є лише однією з усталених дисциплін збору розвідувальної інформації. Стандартного переліку дисциплін збору розвідувальної інформації не існує, однак у розвідувальному співтоваристві США існує консенсус щодо існування п'яти основних дисциплін: HUMINT, SIGINT, IMINT/GEOINT, MASINT [2], і звичайно OSINT. Варто зазначити, що деякі з цих дисциплін (або їх піддисциплін) використовуються виключно державними установами, особливо у сфері воєнної та спеціальної розвідки.

Приватні компанії головним чином розглядають застосування сучасних інструментів OSINT як ефективний спосіб ідентифікації зовнішньої інформації та виявлення внутрішніх активів, що перебувають у відкритому доступі.

У подальших дослідженнях розглядатиметься саме розвідка на основі відкритих джерел – OSINT, адже застосування даного методу може допомагати організаціям зменшити бізнес-ризики й фінансові втрати шляхом збору даних у видимій частині Інтернету й у даркнеті, моніторити у реальному часі інформацію щодо можливих атак, ідентифікувати певні внутрішні загрози компанії.

Література

1. Електронна енциклопедія Wikipedia. Англомовна версія. URL: http://en.wikipedia.org/wiki/Open-source_intelligence
2. Intelligence Studies: Types of Intelligence Collection. URL: https://usnwc.libguides.com/c.php?g=494120&p=3381426.