УДК 004.056 https://doi.org/10.30837/IYF.PCEIP.2024.147

ТАКТИЧНА РОЗВІДКА ЗАГРОЗ В УМОВАХ КІБЕР ВІЙНИ

Пічієнко М. Г.
Науковий керівник – проф. Радівілова Т.А.
Харківський національний університет радіоелектроніки, Харків, Україна
e-mail: mariia.pichiienko@nure.ua, +380961690863

The thesis discusses the effective protection of organisations against digital threats, in particular in the context of cyber warfare and cyber threats affecting Ukrainian companies. The document emphasises the importance of tac-tical threat intelligence and a system of general threat intelligence to prevent and mitigate cyber attacks. The document also discusses the low level of threat intelligence use in Ukrainian organisations due to low awareness, lack of maturity, lack of a comprehensive approach and insufficient community interaction.

Ефективний захист активів організації від цифрових загроз складається з низки задач, серед яких є як аналіз внутрішньої інфраструктури з метою виявлення можливих точок вразливості, так і розуміння потенційних загроз. У останньому випадку команді інформаційної безпеки необхідно мати більш глибоке уявлення, ніж просто поверхнева ідентифікація. Для передбачення та послаблення наслідків від кібератак вони потребують тактичної розвідки загроз — конкретної інформації про тактику, яку цифрові супротивники можуть використовувати для проникнення в систему захисту. [1]

Особливої актуальності розвідка загроз набуває для українських організацій, які є постійними цілями з боку російських APT в умовах російсько-української кібервійни. З 2014 року Україна стала полігоном для випробування кіберпотужностей росії, надаючи можливість іншим спостерігати і дізнаватися про їхню тактику і методи. Російські групи спрямовують свої атаки з метою викрадення інформації, припинення нормального функціонування ресурсів, а також завдання репутаційної шкоди. [2] На даному етапі можна стверджувати, що кібервійна не має кордонів, адже від неї значною мірою потерпають і країни Європи. [3]

Поняття тактичної розвідки загроз вписується в ширшу систему розвідки загроз, в якій різні види інформації про цифрові ризики збираються, аналізуються і передаються зацікавленим сторонам. Ця система включає чотири види розвідки загроз - стратегічну, тактичну, оперативну і технічну - з чіткими відмінностями між ними.

1. Стратегічна розвідка загроз має справу з інформацією високого рівня про мінливий ландшафт цифрових ризиків і про те, як ці зміни можуть вплинути на стан кібербезпеки організації та її готовність до них. Стратегічна розвідка зосереджується на новітніх типах загроз і супротивників, які можуть

становити ризик для організації. Вона найчастіше надається керівництву з метою прийняття стратегічних рішень.

2. Тактична розвідка загроз обробляє конкретну інформацію про новітні тактики, техніки, методи і процедури, які використовують цифрові супротивники для досягнення своїх цілей. Тактична розвідка загроз найчастіше надається керівникам SOC, оскільки вона дозволяє їм впроваджувати відповідні заходи протидії новим моделям атак.

3. Оперативна розвідка загроз є ще більш специфічною, ніж тактична, оскільки вона зосереджена на наданні практичної інформації про ідентифіковану атаку на організацію. Оперативна розвідка найчастіше надається керівникам з мережевої безпеки та їхнім командам, які можуть негайно використовувати цю інформацію в процесі реагування на інциденти.

4. Технічна розвідка загроз фокусується на конкретних індикаторах загроз або індикаторах компрометації (IoC), які сигналізують про зловмисну активність в мережі або системі. Дані про технічні загрози зазвичай передаються групам безпеки, які можуть розпочати розслідування, щоб визначити, чи відбулася атака.

Зазвичай джерелами даних тактичної розвідки загроз виступають:

- обмін інформацією про інформаційну безпеку серед спільноти;
- бази даних про загрози і відкриті джерела (MITRE ATT&CK, публічні threat intelligence feeds, оголошення та попередження про загрози від урядових організацій, таких як CERT-UA в Україні і CISA у США);
- розвідка у DarkNet (аналіз як і скомпроментованих даних організації, так і можливе отримання інформації про майбутні кібератаки у специфічних форумах, каналах, чатах);
- моніторинг публічної площини атак за допомогою спеціалізованих рішень з threat intelligence. [1]

Для українських організацій напрямок розвідки загроз не є широко розвинутим, хоча його актуальність є беззаперечною. Відповідальним за роботу в цьому напрямку на державному рівні є CERT-UA при Державній службі спеціального зв’язку і захистом інформації, в основні задачі якого входить реагування на кіберінциденти, накопичення та проведення аналізу даних про кіберзагрози, а також міжнародна співпраця за наведеними напрямками. CERT-UA регулярно публікує дані про відомі їм атаки разом з IoC і випускає аналітичні звіти з дослідження російсько-української кібервійни.

Однак проведена робота не може бути ефективною без правильної обробки отриманої інформації всередині самих організацій. Наразі загальний рівень threat intelligence в українських організаціях залишається незадовільним через низку чинників.

1. Низький рівень обізнаності. Для багатьох представників організацій threat intelligence обмежується збиранням threat intelligence feeds без їх

подальшої обробки. Розвідка загроз завершується підписанням на розсилки від CERT-UA і переглядом тематичних груп у Telegram у вільний час. Немає уявлення щодо можливості використання даних про загрози у планах стратегічного розвитку і їх інтеграції в системи захисту.

2. Низький рівень зрілості. Використання threat intelligence – це метод проактивного захисту, на той час як більшість українських організацій використовують скоріш реактивний підхід, тобто займаються усунення недоліків інформаційної безпеки вже після того, як відбувся інцидент.

3. Відсутність комплексного підходу. Використання тактичної розвідки про загрози вимагає побудованих процесів у напрямках моніторингу і реагування на інциденти. У найкращому варіанті це має бути повноцінний SOC, який наразі є у великих комерційних компаніях. Йдуть процеси щодо створення окремих галузевих SOCів для низки організацій критичної інфраструктури, але ситуація для державного сектору залишається незадовільною.

4. Низький рівень спілкування. В Україні все ще відбувається процес налагодження культури обміну інформації у сфері кібербезпеки. На жаль, багато організацій продовжують замовчування інцидентів безпеки через боязнь подальших ускладнень, можливих збільшень перевірок з боку регулятора, тощо. Через це багато даних про атаки залишаються невідомими для спільноти.

Отже, ефективний захист активів організації від цифрових загроз є комплексною задачею, в яку повинно входити використання даних про кіберзагрози. В умовах кібервійни це стає все більш актуальним не лише для України, але й країн-партнерів. Побудова налагоджених процесів з обміну даних і проактивний підхід до кіберзагроз є критичним у протистоянні агресії. Українським організаціям необхідно буде підвищувати рівень обізнаності, розвивати використання threat intelligence, впроваджувати комплексний підхід до захисту, а також сприяти обміну інформацією в галузі кібербезпеки. Тільки таким чином можна ефективно стояти на захисті в умовах постійно зростаючого ризику цифрових загроз.

Список використаних джерел

1. What is Tactical Threat Intelligence / Zerofox, 2022. URL: https://www.zerofox.com/blog/what-is-tactical-threat-intelligence/(дата звернення: 24.02.2022)

2. Russia’s Cyber Tactics: Lessons Learned in 2022 / State Service of Special Communication and Information Protection of Ukraine, 2022. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=53466 (дата звернення: 24.02.2022)

3. 2022-2023: A year of Cyber Conflict in Ukraine / Thales, 2023. URL: https://bo-cyberthreat.thalesgroup.com/sites/default/files/2023-03/A%20year%20of%20Cyber%20Conflit%20in%20Ukraine_CTI-2023.pdf (дата звернення: 24.02.2022)