MCIT
Modeling, control & information technologies

Аналіз моделі прогнозування кіберзагроз «Cyber Kill Chain»

https://doi.org/10.31713/MCIT.2024.063

Василь Сус
Поліський національний університет
Житомир, Україна
Sus14012002@gmail.com

Анотація **— Робота присвячена моделі Cyber Kill Chain, розробленій Lockheed Martin для аналізу та протидії кіберзагрозам. Модель включає ключові елементи кібератак, від розвідки до дій на об'єкті. У тезі розглянуто основні методи зловмисників і відповідні заходи захисту на кожному етапі. Обговорено переваги моделі, та її недоліки щодо нових типів загроз. Модель сприяє системному підходу до кібербезпеки і проактивному захисту.**

Ключові слова — Cyber Kill Chain, кібератаки, захист, загрози, етапи атаки, контрзаходи, вразливості, кібербезпека.

ІЗ появою нових IT-технологій зростає інтенсивність нових кібератак на IT-системи. Кібератаки стають все більш витонченими та поширеними. Розуміння методів, які використовують зловмисники, має вирішальне значення для розробки ефективних стратегій захисту. Cyber Kill Chain є одним із таких фреймворків, який допомагає аналізувати кіберзагрози та реагувати на них.

У цій тезі ми розглянемо етапи Cyber Kill Chain, найкращі методи, які використовують зловмисники, і стратегії пом'якшення наслідків для захисту від кібератак.

Cyber Kill Chain — це модель, розроблена компанією Lockheed Martin у 2011 році. В умовах зростаючого числа складних кібератак і появи нових типів загроз компанії потребували систематизованого підходу до аналізу та протидії атакам. Lockheed Martin застосувала концепцію kill chain (ланцюг знищення), що використовується у військових операціях для опису послідовності дій, необхідних для успішного нападу на противника. Військовий ланцюг складався з етапів розвідки, націлювання, атак і завершення місії.

Модель Cyber Kill Chain, є частиною концепції Intelligence Driven Defense для ідентифікації та запобігання кіберзагрозам. Модель була представлена таким чином, що складається з семи етапів: розвідка, озброєння, доставка, експлуатація, встановлення, командування та контроль та дії на об’єкті [1].

Таблиця 1- Етапи моделі Cyber Kill Chain

№	Етапи	Опис
1	Розвідка	Дослідження,ідентифікація та вибір цілей для атаки
2	Озброєння	Підготовка зброї для атаки за допомогою автоматизованих інструментів
3	Доставка	Доставка кіберзброї до цільової системи
4	Експлуатація	Активація кіберзброї
5	Встановлення	Встановлення шкідливого програмного забезпечення на цільовій системі
6	Командування та контроль	Встановлення каналу для віддаленого управління цільовою системою
7	Дії на об’єкті	Досягнення кінцевих цілей (збір інформації, знищення системи тощо)

У компанії Lockheed Martin кібератака проходить через серію чітко визначених етапів або процесів, кожен з яких є необхідним для успішного завершення атаки. Якщо захисник зможе заблокувати хоча б один із цих кроків, зловмисник не зможе перейти до наступного етапу, що порушить всю атаку і зробить її неефективною. Цей підхід базується на ідеї про те, що кібератаки — це складні та багатоступеневі операції, які потребують точного виконання кожного етапу для досягнення мети. Відповідно, кожен етап атаки — від збору інформації та підготовки інструментів до встановлення контролю і виконання злочинних дій — може бути ціллю для контрзаходів.

Для кожного етапу моделі “Cyber Kill Chain” компанії Lockheed Martin існують відповідні контрзаходи, які можуть ефективно зупинити атаку. На етапі розвідки важливо використовувати системи виявлення вторгнень (IDS) та моніторинг мережевого трафіку для виявлення підозрілої активності. На етапі озброєння необхідно мати актуальне антивірусне програмне забезпечення та регулярно оновлювати системи безпеки. Доставка шкідливого програмного забезпечення може бути заблокована за допомогою фільтрації електронної пошти та використання брандмауерів. Експлуатація вразливостей може бути запобігнута впровадженням патчів безпеки та обмеженням прав доступу. Встановлення шкідливого програмного забезпечення можна запобігти за

допомогою антивірусного програмного забезпечення та моніторингу систем. На етапі командування та контролю важливо використовувати системи виявлення вторгнень та моніторинг мережевого трафіку. Нарешті, на етапі дій на об'єкті необхідно використовувати системи виявлення вторгнень (IDS), моніторинг систем та навчання співробітників щодо безпеки. На рисунку 1 зображенно впровадження контрзаходів в моделі Cyber Kill Chain на етапі Експлуатації та розвиток поточної кібератаки на основі моделі.

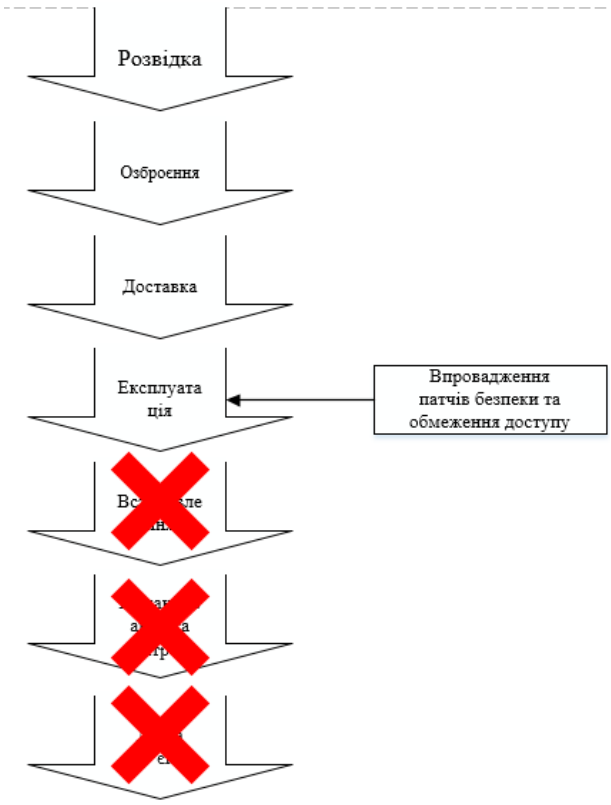

Рисунок 1 Впровадження контзаходів в моделі Cyber Kill Chain

До переваг моделі Cyber Kill Chain можна віднести чітку структуру процесу кібератаки, що дозволяє систематично аналізувати загрози та забезпечувати ефективні заходи для їхнього блокування на кожному з етапів. Модель сприяє проактивному підходу до захисту, що дає змогу запобігати атакам до того, як вони завдадуть шкоди. Крім того, вона дозволяє організаціям краще зрозуміти тактики зловмисників та забезпечити координацію між різними підрозділами з кібербезпеки.

Серед недоліків можна виділити те, що модель орієнтована на відомі типи атак і може бути менш ефективною проти нових, інноваційних загроз, які використовують інші методи або обходять стандартні етапи. Крім того, деякі зловмисники можуть модифікувати свої техніки для уникнення виявлення на етапах, описаних у моделі, що ускладнює своєчасне реагування.

Висновок

Модель Cyber Kill Chain є потужним інструментом та надає організаціям можливість проактивного підходу до безпеки, оскільки кожен етап моделі допомагає виявляти слабкі місця в системах захисту та прогнозувати потенційні загрози. Шляхом детального аналізу кожного етапу атаки, модель дає змогу передбачати, які методи зловмисники можуть використовувати, і створювати відповідні засоби захисту. Вона також допомагає організаціям зосередитися на послідовному вдосконаленні своїх заходів кібербезпеки, орієнтуючись на конкретні етапи кіберзагроз, що підвищує стійкість до атак.

Література

1. Lockheed Martin, The Cyber Kill Chain. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
2. Протидія кіберзагрозам URL: Як протидіяти кіберзагрозам та захистити системи від ворожих кібератак – важливі рекомендації та допомога CERT-UA | Кабінет Міністрів України (kmu.gov.ua)
3. Pols, Paul (17 травня 2021). The Unified Kill Chain. UnifiedKillChain.com.