УДК 004.056.5
Сташук Д.А.[1], Зайко Т.А.[2]
[1] студ. гр. КНТ-228 НУ «Запорізька політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька політехніка»

СПОСОБИ МОДЕЛЮВАННЯ КІБЕРАТАК У СУЧАСНОМУ КІБЕРПРОСТОРІ

Безумовно, будь-яка систематизація починається з аналізу поточних досягнень в даному напрямку: що про це вже говорять авторитетні джерела, що є в найкращих практиках (але про них трохи пізніше).

Модель допомагає діяти ефективніше, тобто не вигадувати велосипед кожен раз і не витрачати дорогоцінні ресурси на зведення воєдино розрізнених результатів або надлишкові кроки. Також система дозволяє швидше залучати до її реалізацію нових учасників, що особливо актуально зараз, при дефіциті готових ІБ-фахівців і необхідності вирішувати багато питань в режимі ASAP.

Сама ж модель [1] повинна бути, по-перше, легко сприймається і по можливості мати графічне представлення, а по-друге, інваріантної до зміни цілей і засобів атакуючих, тому що в іншому випадку потрібно буде кожного разу її переробляти.

Найпопулярнішою атакою є фішинг. Етапи:

– підготовка: формування і стилізація тексту листа і посилання / вкладення, з використанням exploit builder і т.п., з подальшим розсиланням по списку одержувачів;

– отримання доступу: проходження користувачем за посиланням або запуск макросу у вкладенні – запуск dropper;

– виконання завдання / дії: доставка «корисного навантаження»;

– приховування слідів присутності: видалення dropper.

Спіральна модель кібератаки.

Практика показує, що кібератака часто не обмежується одноразовим послідовним проходженням по зазначеним вище етапах. Її реалізація розвивається швидше по спіралі: потрібно виконати одне завдання, перш ніж приступити до іншого.

Дана модель відповідає і досить популярною сьогодні схемою [2], коли один атакуючий отримує доступ, оглядається, а потім продає зібрану інформацію або отриманий доступ іншому непроханого гостя, що переслідують свої цілі і реалізує свої дії.

Чотири методи моделювання загроз.

Процес моделювання кіберзагроз є динамічним і триває протягом усього життєвого циклу розробки програмного забезпечення.

1. Моделювання системи і прийняття рішення про масштаб оцінки.

Першим кроком є створення моделі того, що ви досліджуєте.

Кожен вибір супроводжується своїм набором нових потенційних загроз.

2. Визначення потенційних загроз і атак.

Команда з кібербезпеки намагається уявити собі тип зловмисника, який може спробувати нанести шкоду додатком. Вони намагаються представити,

як кіберзлочинець проводитиме кібератаки. Атаки можуть бути будь-якими - від крадіжки конфіденційних даних до проведення фішинговою атаки або DoS-атаки (відмову в обслуговуванні).

Крім кіберзлочинців, протоколи безпеки також перехоплюють несанкціонований доступ [3]. Якісна система моделювання загроз повинна захищати програмне забезпечення як від кібератак, так і від ненавмисних помилок.

3. Проведення аналізу загроз.

Проведення аналізу загроз – довгий і трудомісткий процес. Контрольний список або шаблон спрямований на досягнення однаковості при кожному тестуванні безпеки. Він допомагає розробникам перевірити кожен шлях на наявність різних шкідливих загроз, таких як спуфинг, відмова в обслуговуванні і підвищення привілеїв.

4. Визначення пріоритетів потенційних загроз.

Після того як всі потенційні загрози визначені і задокументовані, настав час розставити пріоритети. Не кожна загроза з однаковою ймовірністю може призвести до серйозного збитку, наприклад, до витоку даних. Тут на допомогу приходить знання статистики кібератак.

При визначенні пріоритетів загроз експерти з кібербезпеки повинні оцінити ймовірність і наслідки кожного типу атак.

Моделювання загроз і методи їх усунення.

Заключним етапом моделювання кіберзагроз [4] є визначення та пропозиція контрзаходів. Експерти з кібербезпеки використовують всі зібрані дані для зниження ризиків безпеки до прийнятного рівня. Широкий спектр методів усунення загроз може допомогти пом'якшити задокументовані загрози. Експерти зазвичай складають звіт, що містить практичні кроки по захисту програмного забезпечення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Сердюк В.А. Анализ современных тенденций построения моделей информационных атак / В.А. Сердюк // Информационные технологии. – 2004. – № 5. – С. 94–101.

2. Коломеец М.В. Методика визуализации метрик кибербезопасности / М.В. Коломеец, А.А. Чечулин, Е.В. Дойникова, Котенко И.В. // Изв. вузов. Приборостроение. – 2018. – Т. 61, № 10. – С. 873–879.

3. Kotenko I.V. The use of attack to evaluate the security of computer networks and analysis of security events. High Availability Systems / I.V. Kotenko, A.A. Chechulin. – 2013. – Vol. 9, no. 3. – P. 103–110.

4. Massimiliano Albanese A Graphical Model to Assess the Impact of Multi-Step Attacks / Massimiliano Albanese, Sushil Jajodia // Journal of Defense

Modeling and Simulation: Applications, Methodology, Technology. – 2018. – Vol. 15(1). – P. 79–93.