УДК 004.4:004.056.5

КЛЮЧОВІ ЗАСАДИ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В УМОВАХ СУЧАСНИХ ЗАГРОЗ ЗА ДОПОМОГОЮ ФРЕЙМВОРКУ МАТРИЦІ MITRE ATT&CK

Гребєнік О. А.
Науковий керівник – асистент Гвоздьов Р. Ю.
Харківський національний університет радіоелектроніки, каф. БІТ
м. Харків, Україна
e-mail: oleksandr.hrebienik@nure.ua

In today's digitally interconnected world, ensuring cybersecurity and safeguarding software have become paramount. This abstract delves into the fundamental principles of cybersecurity and software protection amidst contemporary threats, emphasizing the utilization of the Mitre Matrix framework. The Mitre Matrix framework provides a structured approach to understanding and mitigating cyber threats by categorizing them into various attack tactics and techniques. It discusses how the Mitre Matrix framework aids in identifying, analyzing, and responding to cyber threats effectively. Ultimately, integrating the Mitre Matrix framework into cybersecurity strategies empowers organizations to adapt to dynamic threat landscapes and safeguard their digital assets effectively.

Розглядаючи постійний розвиток цифрового світу і зростання кількості та складності кіберзагроз, стає очевидним необхідність у глибшому аналізі принципів та методів кібербезпеки. Одним із найбільш ефективних інструментів, що допомагає в цьому, є фреймворк MITRE ATT&CK. Він надає систематизований підхід до класифікації кіберзагроз, що сприяє кращому їх розумінню та аналізу.

У світі постійно змінюються підходи до кібербезпеки, і важливо бути в курсі останніх тенденцій та інструментів для ефективного захисту цифрових активів. Фреймворк MITRE став одним з таких інструментів, який дозволяє експертам з кібербезпеки систематизувати та аналізувати різноманітність кіберзагроз. За допомогою цього фреймворку, спеціалісти із захисту інформації можуть краще розуміти методи та тактики атак, що використовуються зловмисниками, та відповідно реагувати на них.

Один із ключових аспектів, який варто підкреслити при вивченні фреймворку MITRE, є його здатність до глибокого аналізу різних типів кіберзагроз за допомогою класифікації за конкретними тактиками та техніками атак.

Наприклад, розглянемо техніку фішинга – матриця MITRE дозволяє систематизувати цю загрозу, а також надає короткий опис, приклади процедур і заходи пом’якшення. Детальне вивчення таких конкретних випадків допомагає розібратися у специфіці кожної загрози та визначити оптимальні заходи захисту.

Крім того, важливою перевагою MITRE є здатність до ефективного виявлення потенційних кіберзагроз. За допомогою даного фреймворку можна виявити слабкі місця в системі та потенційні шляхи атаки, що надає можливість вчасно реагувати та запобігти можливим інцидентам інформаційної безпеки.

Інтеграція фреймворку MITRE в концепції та стратегії кіберзахисту відкриває широкі можливості для організацій у сфері захисту інформації. Наприклад, порівняльний аналіз з іншими фреймворками дозволяє виявити переваги та недоліки кожного з них, а це допомагає у створенні більш комплексної та ефективної стратегії захисту. Використання фреймворку також впливає на розвиток проактивних підходів до кібербезпеки, що дозволяє уникати більшості потенційних загроз та мінімізувати можливі збитки. Наприклад, впровадження фреймворку може змусити організацію регулярно проводити аудит безпеки, вдосконалювати політику паролів та багато іншого, що сприяє підвищенню загального рівня кібербезпеки.

Ще однією важливою складовою є здатність фреймворку до гнучкості та адаптабельності. Він може бути використаний для аналізу різноманітних типів кіберзагроз і захисту, включаючи атаки на додатки, мережеві проникнення та соціальну інженерію. Це робить фреймворк універсальним і підходящим для різних сфер та галузей, що стикаються з кіберзагрозами.

У великих організаціях, де є наявність великої кількості ресурсів та експертів з кібербезпеки, фреймворк MITRE може бути дуже корисним інструментом для аналізу та захисту від кіберзагроз. Його використання може допомогти організаціям ідентифікувати та вирішувати потенційні загрози, що дозволить збільшити рівень кібербезпеки та знизити ризики для бізнесу. Однак, перед впровадженням фреймворку необхідно ретельно оцінити його потенційні переваги та обмеження для конкретної організації.

Загалом, фреймворк MITRE є важливим інструментом для розуміння, аналізу та реагування на кіберзагрози. Використання цього інструменту в комплексі з іншими методами кібербезпеки сприяє підвищенню ефективності захисту та забезпечує безпеку цифрових активів в умовах постійно зростаючих загроз. Порівняльний аналіз, детальні приклади та інтеграція з іншими інструментами дозволяють вдосконалити стратегії захисту.

Список використаних джерел:

1. MITRE ATT&CK®. MITRE ATT&CK®. URL: https://attack.mitre.org/ (дата звернення: 03.03.2024).

2. Georgiadou, A., Mouzakitis, S.; Askounis, D, Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework. Sensors 2021, 21, 3267. URL https://doi.org/10.3390/s21093267.