УДК 004.002

МЕТОДОЛОГІЯ ОЦІНКИ ZERO TRUST

ZERO TRUST EVALUATION METHODOLOGY

Володимир Гаращенко, Новосад Катерина

Волинський національний університет імені Лесі Українки, просп. Волі, 13, Луцьк, 43025, Україна

Abstract. *This work examines the methodologies for Zero Trust assessment, which include risk analysis to assess current threats and vulnerabilities and the use of metrics to assess performance.*

У сучасних умовах кібербезпеки традиційні методи захисту виявляються недостатніми. Zero Trust (нульова довіра) – це підхід, що базується на принципі "нікому не довіряй, все перевіряй". Він передбачає постійну перевірку всіх користувачів та пристроїв, незалежно від їхнього розташування в мережі. Для аналізу ефективності архітектури нульової довіри можна використовувати різні математичні моделі. Деякі з них також допомагають запобігти бічним рухам в архітектурі з ZT. Вони використовують дуже складні алгоритми та рівняння для посилення та покращення безпеки мереж. Дві найбільш відомі математичні моделі для аналізу ефективності нульової довіри – це моделі запобігання бокового руху та виявлення загроз. Модель бокового запобігання розроблена для оцінки та пом’якшення поширення кіберзагроз у мережевому середовищі після злому. Формула показує, як розраховується зменшення бічного руху:

Зменшення бічного руху = (початкові спроби бічного руху – остаточні спроби бічного руху) / (початкові спроби бічного руху) x 100% (1)

Модель виявлення загрози можна визначити як математичну модель, спеціально розроблену для виявлення потенційних кіберзагроз і реагування на них в межах мережі. Формула 2 показує, як розраховується коефіцієнт виявлення загроз.

Швидкість виявлення загроз = (Кількість Виявлені загрози) / (Загальна кількість загроз) x 100% (2)

Модель байєсівської мережі пропонує імовірнісний графічний підхід до представлення невизначених знань про стан мережі та залежності між різними змінними. Байєсівський висновок може оцінити ймовірність порушень безпеки та полегшити прийняття рішень щодо стратегій зменшення ризиків. Формула 3 показує, як це обчислити.

$$(A|B) = \frac{P(B|A)P(A)}{P(B)} \quad (3)$$

Модель теорії ігор забезпечує основу для аналізу стратегічної взаємодії між кількома об’єктами в мережевому середовищі. Модель теорії ігор забезпечує основу для аналізу стратегічних взаємодій між кількома об'єктами в мережевому середовищі. Теорія ігор використовується для вивчення природи кіберінцидентів у сфері кібербезпеки, оскільки мережеві захисники, зловмисники та користувачі взаємодіють для досягнення результатів. Теорія ігор корисна для моделювання поведінки та стратегії кожного гравця та врахування взаємодії між гравцями, з якими потрібно грати. Нарешті, модель ланцюга Маркова, представляє послідовність подій, у якій ймовірність кожної події залежить лише від стану,

досягнутого попередньою подією. У контексті ZTA моделі ланцюга Маркова моделюють розвиток загроз безпеці та аналізують ймовірність бокового руху в мережі з часом, допомагаючи зрозуміти динаміку кіберзагроз і оцінюючи ефективність впровадження ZTA.

Математичні моделі є важливим інструментом для аналізу ефективності підходу Zero Trust у кібербезпеці. Вони дозволяють формалізувати складні процеси та взаємодії в інформаційних системах, забезпечуючи кількісну оцінку ризиків і ефективності впровадження заходів безпеки. За допомогою цих моделей можна оцінювати ймовірність успішних атак, прогнозувати потенційні втрати, а також визначати оптимальні стратегії захисту.

Бібліографія

1. Ahmadi S. Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities. Journal of Engineering Research and Reports. 2024. Vol. 26, no. 2. P. 215–228. URL: https://doi.org/10.9734/jerr/2024/v26i21083 (date of access: 21.05.2024).

2. Irei A., Shea S. What is the Zero-Trust Security Model. Security. URL: https://www.techtarget.com/searchsecurity/definition/zero-trust-model-zero-trust-network (date of access: 21.05.2024).