УДК: 004.415.3

МАТЕМАТИЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ МОНІТОРИНГУ ЗАХИЩЕНОСТІ МЕРЕЖЕВИХ СИСТЕМ

Маланчук В.М., Столяр О.Й., Гуменюк М.Б.
Західноукраїнський національний університет
магістранти

I. Постановка проблеми

Підхід до оцінки захищеності КС та вибору захисних заходів, заснований на комплексній системі показників та алгоритмів їх обчислення із застосуванням графів атак та графів залежностей сервісів, які дозволять враховувати різні характеристики комп'ютерних атак, а також різні аспекти функціонування системи, що захищається і вибирати найбільш ефективні захисні заходи, в цілому призведе до суттєвого підвищення ефективності реагування на інциденти атак, що допоможе підвищити захищеність програмних продуктів та процесів. Таким чином, завдання розробки такого підходу є актуальним.

II. Мета роботи

Мета даної роботи полягає у підвищенні захищеності веб-орієнтованих систем за рахунок удосконалення методик, моделей та алгоритмів оцінки захищеності та вибору контрзаходів з урахуванням обчислення показників захищеності.

III. Обґрунтування отриманих результатів

Проаналізовано процес менеджменту ризику інформаційної безпеки та визначено місце оцінки та обробки ризику, виділено основні етапи даних процесів. Визначено, що для системи організацій, для яких ІТ є критичними, кращою є детальна кількісна оцінка ризику. Обґрунтовано необхідність створення нових методик оцінки та обробки ризику на основі комплексного аналізу даних з різних джерел. Визначено вимоги до методик, що розробляються. Розроблено комплекс показників захищеності, що включає у собі окремі показники та зв'язки між ними. Основною відмінністю запропонованого комплексу є ієрархічний спосіб класифікації показників. Класифікація здійснюється на основі вхідних даних, що застосовуються для обчислення показників, етапів процесу аналізу ризиків та значень показників. Розроблено методику оцінки захищеності на основі графів атак та залежностей сервісів та запропонованого комплексу показників. Основною відмінністю методики є ієрархічний характер, що відповідає рівням комплексу показників, що дозволяє в залежності від наявних вхідних даних отримати оцінку поточної ситуації із захищеності, виражену у формі адекватних кількісних показників і уточнювати оцінку з появою нових даних.

Висновок

Оцінка захищеності та вибір захисних заходів на основі адекватних кількісних показників є важливим та актуальним завданням інформаційної безпеки. В роботі розроблено модель, методику та алгоритми для оцінки захищеності системи та вибору захисних заходів для систем моніторингу безпеки та управління інцидентами, застосування яких призведе до підвищення ефективності процесу оцінки захищеності та вибору контрзаходів.

Розроблено архітектуру та програмну реалізацію системи оцінки захищеності системи та вибору захисних заходів. Основною відмінністю є застосування оригінальних методик оцінки захищеності та вибору захисних заходів.

Список використаних джерел

1. Li, Z.; Zhao, Y.; Li, Y.; Rahman, S.; Yu, X.; Zhang, J. Demonstration of Fault Localization in Optical Networks Based on Knowledge Graph and Graph Neural Network. In Proceedings of the Optical Fiber Communications Conference and Exposition (OFC 2020), San Diego, CA, USA, 8–12 March 2020; pp. 1–3.
2. Gray, W.; Tsokanos, A.; Kirner, R. Multi-Link Failure Effects on MPLS Resilient Fast-Reroute Network Architectures. In Proceedings of the International Symposium on Real-Time Distributed Computing (ISORC 2021), Daegu, Korea, 1–3 June 2021; pp. 29–33.
3. Dusia, A.; Sethi, A.S. Recent Advances in Fault Localization in Computer Networks. IEEE Commun. Surv. Tutor. 2016, 18, 3030–3051.
4. Ab-Rahman, M.S.; Chuan, N.B.; Safnal, M.H.G.; Jumari, K. The overview of fiber fault localization technology in TDM-PON network. In Proceedings of the International Conference on Electronic Design, Penang, Malaysia, 1–3 December 2008; pp. 1–5.