Міжнародна науково-практична конференція
«ЕНЕРГЕТИЧНІ УСТАНОВКИ ТА АЛЬТЕРНАТИВНІ ДЖЕРЕЛА ЕНЕРГІЇ»
(ESAES – 2024)
11-12 березня 2024 року

Секція:
Наукові дослідження, діагностика, випробування, експлуатація та надійність енергосистем. Оптимізація результатів дослідження

ПРОБЛЕМАТИКА ПОБУДОВИ ПРОГРАМНО-КОНФИГУРОВАННИХ МЕРЕЖ

Плєхова Ганна Анатоліївна,
кандидат технічних наук, доцент,
завідувач кафедри інформатики та прикладної математики,
Харківський національний автомобільно-дорожній університет

Костікова Марина Володимирівна,
кандидат технічних наук, доцент

Козачок Лариса Миколаївна,
старший викладач кафедри інформатики та прикладної математики, Харківський національний автомобільно-дорожній університет

Вступ

В роботі проведено аналіз щодо вразливостей площини даних SDN, розглянуті функціональні можливості засобів маршрутизації протидії можливим атакам, показана перспективність використання засобів безпечної маршрутизації. Аналіз засобів проведено на основі базових метрик критичності вразливостей, вони в свою чергу використовуються для підвищення рівня мережної безпеки площини даних SDN. Проведено аналіз стандарту CVSS, проаналізований кількісний розрахунок рівня вразливості мережного обладнання, показано доцільність його використання під час розробки та дослідження перспективних підходів до безпечної маршрутизації у площині даних SDN (Software-Defined Networking, SDN).

Розглянути підходи до проектування та побудови програмно-конфігуровані мережі (Software-Defined Networking, SDN) та їх експлуатації. Основні підходи для інфокомунікаційних мереж базуються на тому, що шляхом розділення площин управління (controlplane) та передавання даних (dataplane) ми досягаємо бажаного ефекту: такий розподіл надає мережі безпосередньої програмованості та динамічності; дозволяє абстрагувати функціональні можливості рівня інфраструктури.

NFV

Віртуалізація мережних функцій (Network Functions Virtualization, NFV) є стандартизованим способом для розробки, впровадження та керування мережними службами. NFV використовує концепцію, яка передбачає заміну спеціальних пристроїв мережної інфраструктури. Проводимо заміну маршрутизаторів та брандмауерів – стандартними серверами, комутаторами, сховищем та хмарою. Можливо навіть використовувати туманну обчислювальну інфраструктуру. NFV відокремлює функції мережі, такі як маршрутизація, комутація та безпека від виділених апаратних пристроїв або пропрієтарних и це дозволяє їм працювати в межах програмного забезпечення.

Використання NFV працює таким чином що головною метою є те, щоб використовувати стандартні технології віртуалізації для консолідації апаратного забезпечення. Крім того це дозволяє проводити віртуалізацію мережних функцій у блоки, які в свою чергу можна об’єднувати для створення наскрізних комунікаційних послуг. Така реалізація можлива для будь-якої функції площини управління або площини даних. Причому можливо використовувати як середовище дротяних мереж так і без дротяних.

Основних компоненти NFV: VNF, NFVI, MANO.

Основні вимоги щодо безпеки NFV, SDN і хмарних технологій

Для забезпечення безпеки об’єкта необхідно забезпечити п’ять основних функцій безпеки CIAAA:

- конфіденційність (Confidentiality);
- цілісність (Integrity);
- доступність (Availability);
- автентичність (Authenticity);
- підзвітність (Accountability).

Ключові елементи кіберпростору:

- реальні та віртуальні об’єкти (сутності) ;
- інфраструктура взаємозв’язку (комунікацій);
- взаємодія між об’єктами через інфраструктуру.

Кібербезпека пов’язана з виявленням вразливостей кіберпростору.

Оцінка ризику, пов’язаного із загрозою, сприяє розробці нових рішень щодо безпеки та формулюванню вимог до цих рішень.

Проблеми безпеки NFV

Оскільки мережні компоненти віртуалізовані, NFV-мережі містять рівень абстракції, якого немає в традиційних мережах. Захист цього складного та динамічного середовища, яке охоплює віртуальні та фізичні ресурси, елементи керування, протоколи, а також границі між віртуальними та фізичними мережами, є складним завданням з багатьох причин:

1) Залежності гіпервізора.
2) Еластичні границі мережі.
3) Динамічні робочі навантаження.
4) Додавання сервісів і служб.
5) Перевірка зі збереженням стану (stateful)/без збереження стану (stateless).
6) Масштабованість доступних ресурсів.

Висновки

Таким чином, SDN представляє собою нову мережну парадигму, а її вплив полягає у формі нової структури, нових компонентів, структурних рівнів та інтерфейсів. SDN несе з собою нові виклики безпеці, які виходять за рамки традиційних мереж. Оскільки SDN відокремлює рівень керування від рівня даних, ця технологія приносить із собою нові набори компонентів, інтерфейсів, а також багато нових питань безпеки.