використати фізичні явища (теплове розширення тіл, оптичні явища інтерференції та дифракції), технічний ефект передачі енергії досягається завдяки використанню фізичних процесів взаємодії тіл, теплопередачі, хвильового руху, явища електромагнітної індукції та ін. Досить часто для оптимізації технічних рішень використовуються різні математичні моделі.

Отже, розв'язуючи творчі технічні задачі, котрі обов'язково містять певні протиріччя, студенти стикаються з необхідністю використовувати свої знання, які вони здобули в школі, у вищому навчальному закладі для практичного вирішення проблем.

Саме такий підхід сприяє усвідомленню здобувачами освіти того, що різні наукові напрямки існують в тісному поєднанні, і знання з фізики, хімії, математики та інших дисциплін мають практичне застосування в інших галузях.

Таким чином, розв'язання творчих технічних задач, використання міждисциплінарного підходу, безперечно, сприяє формуванню творчих здібностей студентів: вміння генерувати ідеї, критично їх оцінювати, вироблення здатності до перенесення досвіду, розвиток цілісності сприйняття дійсності та ін.

Крім того, виконання практичних завдань різного рівня складності стимулює самостійність, відповідальність і здатність до інноваційного підходу, що є важливими складовими професійної підготовки сучасного фахівця.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Козак Л. В. Технології розвитку творчого мислення у професійній освіті / Педагогічні науки. 2021. № 77. С. 112 –1 18.
2. Туров М.П. Основи винахідництва та методи пошуку розвязку творчих технічних задач. Методичний посібник /за ред. В.Ф. Паламарчука. Київ: Освіта України, 2008. 312 с.
3. Щирбул О.М. Удосконалення змісту дисципліни «Технічна творчість» – важливий елемент формування творчого потенціалу студентів Наукові записки /Ред. кол.: В.Ф. Черкасов, В.В. Радул, Н.С. Савченко та ін. Випуск 168. Серія: Педагогічні науки. Кропивницький: РВВ КДПУ імені В. Винниченка. 2018. С. 295 – 297.

ЮЗЕФОВИЧ Юрій

старший викладач, викладач - методист,

завідувач відділення «Інформаційні технології та робототехніки»

Самбірського фахового коледжу економіки та інформаційних технологій

КУЗЬО Андрій

магістрант Західноукраїнського національного університету

ФІЛЬТРАЦІЯ МЕРЕЖЕВОГО ТРАФІКУ В КЛАСТЕРНИХ СЕРЕДОВИЩАХ: ПРОБЛЕМАТИКА ТА СУЧАСНІ ПІДХОДИ

Сучасні кластерні середовища, зокрема платформи контейнерної оркестрації на кшталт Kubernetes, суттєво змінили підходи до побудови та експлуатації розподілених інформаційних систем. Висока щільність розміщення робочих навантажень, динамічне масштабування та абстракція від фізичної

інфраструктури дозволяють ефективно використовувати ресурси, однак водночас ускладнюють питання інформаційної безпеки. Однією з ключових проблем у таких середовищах є фільтрація та контроль мережевого трафіку всередині кластера.

Традиційні підходи до захисту мережі, що базуються на використанні фізичних або апаратних міжмережевих екранів, не завжди є ефективними в умовах сучасних кластерів. Значна частина трафіку залишається невидимою для таких засобів, що створює потенційні вектори атак і підвищує ризики компрометації.

Види мережевого трафіку в кластері

Для аналізу та побудови політик безпеки важливо чітко розрізняти типи мережевого трафіку, характерні для кластерних середовищ. Найпоширенішою є класифікація на east-west та north-south трафік.

- North-south трафік – це трафік, який перетинає межу кластера. До нього належать запити від зовнішніх користувачів або систем до сервісів, що працюють у кластері, а також вихідні з'єднання кластера з зовнішніми ресурсами, наприклад базами даних, API сторонніх сервісів або іншими дата-центрами. Саме цей тип трафіку традиційно добре контролюється за допомогою периметрових фаєрволів, балансувальників навантаження та систем виявлення вторгнень.
- East-west трафік – це внутрішній трафік між компонентами всередині кластера. Він охоплює комунікацію між подами, сервісами та мікросервісами, незалежно від того, чи розміщені вони на одній ноді або на різних. У сучасних мікросервісних архітектурах саме east-west трафік становить переважну частину всіх мережевих взаємодій і є критично важливим з погляду безпеки.

Концепція Zero Trust

Одним із фундаментальних підходів до побудови безпеки в сучасних розподілених системах є концепція Zero Trust. Вона ґрунтується на принципі «нікому не довіряй за замовчуванням», незалежно від того, знаходиться суб'єкт доступу всередині чи поза межами мережевого периметра.

У моделі Zero Trust кожна спроба доступу до ресурсу повинна бути перевірена, автентифікована та авторизована. Довіра не надається автоматично на основі розташування в мережі, IP-адреси або належності до певного сегмента. Для кластерних середовищ це означає необхідність контролю не лише north-south, а й east-west трафіку, з урахуванням ідентичності кожного пода або сервісу та контексту його взаємодії.

Архітектура кластера та обмеження традиційних фаєрволів

Типовий кластер контейнерної оркестрації складається з декількох нод, кожна з яких є окремим фізичним або віртуальним сервером. На кожній ноді може одночасно працювати велика кількість подів, які спільно використовують ресурси операційної системи хоста, зокрема ядро та мережевий стек.

Комунікація між подами, розміщеними на одній ноді, зазвичай відбувається через віртуальні мережеві інтерфейси та програмні мережеві механізми. Такий трафік не виходить за межі ноди і, відповідно, не проходить через фізичні мережеві пристрої. У результаті апаратні фаєрволи опиняються в

«сліпій зоні» та не здатні аналізувати або фільтрувати значну частину внутрішнього трафіку.

У разі компрометації одного пода або сервісу зловмисник може отримати доступ до внутрішнього мережевого простору ноди. За відсутності належної сегментації та контролю це створює серйозну загрозу для всіх інших подів, що працюють на тій самій ноді, та може призвести до ескалації атаки в межах усього кластера.

Фільтрація трафіку на рівні ядра операційної системи

З огляду на обмеження фізичних фаєрволів, актуальним є підхід до реалізації політик безпеки безпосередньо на рівні операційної системи ноди. Одним із сучасних та ефективних інструментів для цього є технологія eBPF (extended Berkeley Packet Filter).

eBPF дозволяє виконувати спеціалізовані програми в ядрі операційної системи без необхідності модифікації самого ядра. За допомогою eBPF можна перехоплювати мережеві пакети, аналізувати їхні характеристики, застосовувати правила фільтрації та збирати телеметрію щодо внутрішнього трафіку між подами. Такий підхід дає змогу реалізувати детальний контроль east-west трафіку, включно з перевіркою протоколів, портів, ідентичності подів та поведінкових патернів. Важливо, що аналіз відбувається на тій самій ноді, де генерується або приймається трафік, що мінімізує затримки та накладні витрати.

Децентралізований аналіз та виявлення аномалій. Окремої уваги заслуговує підхід, за якого кожна нода кластера має власний механізм аналізу трафіку та виявлення аномалій. На відміну від централізованих рішень, які потребують дублювання всього мережевого трафіку на окрему аналітичну ноду, децентралізована модель має низку переваг.

По-перше, зменшується навантаження на мережу, оскільки немає потреби передавати великі обсяги даних для централізованої обробки.

По-друге, підвищується масштабованість системи безпеки: зі збільшенням кількості нод автоматично зростає і загальна обчислювальна потужність для аналізу.

По-третє, локальний аналіз дозволяє швидше реагувати на підозрілу або аномальну активність, ізолюючи проблемний под або ноду без затримок, пов’язаних із централізованою кореляцією подій. Це добре узгоджується з принципами Zero Trust та мінімізації потенційного радіуса ураження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Using eBPF to identify ransomware that use DGA DNS queries. Information Technology and Security. 2023. URL: http://its.iszzi.kpi.ua/article/view/293760

2. Система моніторингу мережевого трафіку у кластері Kubernetes. Вісник Технологічного університету Поділля. URL: https://heraldts.khmnu.edu.ua/index.php/heraldts/article/download/1769/2062/7014