УДК 004.75; 004.7
DOI: 10.31673/2409-7292.2025.012325

Сиротинський Р. М., Тишик І. Я.

ОСОБЛИВОСТІ ПРОЕКТУВАННЯ МІКРОСЕГМЕНТАЦІЇ МЕРЕЖІ ПРИ ПОБУДОВІ АРХІТЕКТУРИ НУЛЬОВОЇ ДОВІРИ

В роботі описані підходи щодо реалізації мікросегментації корпоративної мережі організації з метою забезпечення якісного контролю доступу до елементів її інфраструктури та покращення управління ними. Впровадження мікросегментації мережі для обмеження горизонтального переміщення між елементами її інфраструктури є одним з ключових заходів міграції до архітектури нульової довіри. Мікросегментація забезпечує оптимальну продуктивність мережі та дозволяє ефективно керувати доступом до її ресурсів, як на межі так і в середині мережі. Також надає можливість ізолювати критичні ресурси організації від небезпечних мережних з'єднань, що зменшує ризик несанкціонованого доступу до них.

Актуальність впровадження сучасних безпекових моделей вимагає якісного планування та проектування мікросегментації мережевої інфраструктури. Цей процес спричиняє зміну архітектури мережі та несе за собою як безпекові покращення так і ряд певних недоліків пов'язаних з підвищенням складності топології, та збільшення вартості та складності впровадження, збільшенням витрат на обслуговування та подальшої експлуатації мікросегментованої інфраструктури. В дослідженні аналізуються переваги та недоліки мікросегментації різної гранулярності. Щільна мікросегментація підвищує рівень захищеності корпоративної інфраструктури в цілому при компрометації окремих її елементів в той час як малосегментована мережева інфраструктура не вимагає значних ресурсів, є легкою в операційній підтримці а також в цілому не знижує продуктивність корпоративної мережі. Запропоновано метод аналітичного проектування мікросегментації з використанням матриць ризиків як інструмента оцінки корпоративних систем для визначення необхідного рівня захищеності та вибору необхідного розміру мікросегмента. Розглянуто приклад впровадження мікросегментації в типовій інфраструктурі та різницю в її топології до і після зміни. Проаналізовані причини та потреби оптимізації первинного дизайну мікросегментації. Розглянуто варіанти та підходи виконання оптимізації дизайну мікросегментації корпоративної інфраструктури.

Ключові слова: мікросегментація, нульова довіра, мережа, файрвол, інфраструктура, гранулярність

Вступ

Мікросегментація є методом забезпечення мережевої безпеки, який передбачає поділ мережі на менші ізольовані сегменти (мікросегменти) для застосування конкретних засобів контролю безпеки до кожного сегмента. Цей метод зазвичай використовується для обмеження горизонтального переміщення зловмисників шляхом застосування детальних політик безпеки до окремих робочих навантажень або груп пристроїв. Таким чином, навіть якщо зловмисник отримує доступ до однієї частини мережі, його можливості доступу до інших частин будуть обмежені.

У сучасних реалізаціях, особливо в хмарних середовищах, політики мікросегментації часто автоматично створюються за допомогою динамічних та статичних алгоритмів аналізу для контролю доступу між сервісами на основі законних моделей доступу [1].

Мікросегментація вважається важливою частиною архітектури Zero Trust (ZTA), де вона підвищує рівень безпеки, гарантуючи, що всі внутрішні комунікації піддаються таким самим суворим перевіркам, як і зовнішні, зменшуючи поверхню атаки та обмежуючи потенційну шкоду від порушень безпеки [2].

Аналіз літературних джерел та формулювання проблеми.

Впровадження та проектування мікросегментації згадується авторами сучасних наукових праць достатньо часто. Автори розмірковують над впливом мікросегментації на корпоративну інфраструктуру, пропонують варіанти реалізації та працюють над алгоритмами аналізу, проектування та застосування мікросегментації з використанням різних технологічних рішень.

Ноель та ін. (2021) обговорюють компроміси між безпекою та продуктивністю при проектуванні політик сегментації. Їхнє дослідження показує, що дрібнозерниста мікросегментація, хоча й складніша, значно підвищує стійкість до кібератак, зменшуючи можливості латерального переміщення в межах мережі [3].

Інші дослідження твердять що на практиці мікросегментація підвищує загальний рівень безпеки, не впливаючи суттєво на продуктивність мережі, що робить її ефективною для захищених мереж центрів обробки даних. [4]

Автори Yinqiu Liu та інші в своєму дослідженні пропонують модель ієрархічної мікросегментації на основі графів для оптимізації безпеки та ефективності мережі. Для підвищення точності сегментації пропонується використання алгоритма на базі великих мовних моделей. [5]

Серед опублікованих сучасних праць проведено дослідження про вплив мікросегментації на продуктивність мережі. Автори: Мухаммад Муджиб та Р. Ф. Сарі оцінюють продуктивність мікросегментації в центрах обробки даних за допомогою Cisco Application Centric Infrastructure та вимірюють затримку, тремтіння та втрату пакетів, показуючи, що мікросегментація покращує безпеку без погіршення продуктивності мережі.[6] На їх думку програмно-визначена мережа (SDN) є ключовим засобом для впровадження мікросегментації Zero Trust.

Також в сучасних працях розмірковується над особливостями впровадженя мікросегментації в хмарних оточеннях та пропонується заснований на політиках підхід до перевірки мережевого трафіку на рівнях портів і протоколів, щоб обмежити несанкціоноване спілкування.[7]

Ці публікації надають поглиблене розуміння дизайну, реалізації та продуктивності мікросегментації в архітектурі нульової довіри. Дослідження висвітлює ключові методології, від ієрархічної сегментації на основі графів до реалізацій на основі програмно-визначених мереж (SDN). Разом вони зміцнюють мікросегментацію як фундаментальний захід безпеки, який зменшує бічні рухи, покращує контроль доступу та підвищує безпеку в хмарі, центрі обробки даних і корпоративному середовищі.

В сучасних корпоративних середовищах задача проектування мікросегментації постає з урахуванням індивідуальних особливостей , таких як специфіка корпоративної інфраструктури, вимоги до підвищення захищеності мережі, певний допустимий рівень просідання продуктивності та керованості і також не в останню чергу дотримання витрат в межах бюджету, виділеного на імплементацію.

Яка б стратегія побудови мікросегментації не була обрана за основу - проектування мікросегментації це балансування між захищеністю з однієї сторони та зручністю користування\продуктивністю\вартістю реалізації з іншої. Банально найбезпечніший варіант - кожен окремий хост мережі в окремому сегменті, захищеному контролем доступу, є мало реалістичним сценарієм з огляду на складність реалізації та високу ресурсозатратність в сучасних корпоративних інфраструктурах. З іншого боку формальне впровадження мікросегментації з розподілом однорангової мережі на 2 чи 4 сегменти не дасть відчутного захисту та не відповідатиме принципам нульової довіри. Таким чином при впровадженні або міграції до архітектури нульової довіри постає питання оптимального підходу до проектування мікросегментації який би забезпечував в першу чергу безпекову цінність для інфраструктури та з іншого боку не обтяжував би її надмірною вартістю впровадження, складністю операційної підтримки а також не чинив відчутного впливу на якість мережевих сервісів які надаються.

Мета роботи та цілі дослідження

Метою роботи є дослідження можливості реалізації мікросегментації мережі з різною гранулярністю в корпоративній інфраструктурі організації з точки зору покращення її безпекових характеристик та керованості. Цілями дослідження є вирішення задачі розробки підходів та практик щодо ефективного проектування мікросегментації корпоративної мережі та подальшого її впровадження у мережеву інфраструктуру організації, з урахуванням зростання складності мережевої інфраструктури в рамках побудови архітектури нульової довіри.

© Сиротинський Р. М., Тишик І. Я. (2025). Особливості проектування мікросегментації мережі при побудові архітектури нульової довіри. Сучасний захист інформації, 1(61), 229–240. https://doi.org/10.31673/2409-7292.2025.012325.

Основна частина

Мікросегментація в межах архітектури Zero Trust (ZTA) може бути реалізована за допомогою різних стратегій і підходів, що забезпечують надійний захист шляхом ізоляції мережевого трафіку та впровадження суворих заходів контролю доступу. Ось основні типи та стратегії для впровадження мікросегментації в середовищах Zero Trust:

1. Сегментація на основі ідентичності. Ця стратегія передбачає застосування заходів безпеки на основі ідентичності користувачів, пристроїв або додатків, а не на основі IP-адрес. Кожен сегмент визначається атрибутами ідентичності, що забезпечує доступ лише перевіреним і автентифікованим суб'єктам. Такий підхід обмежує латеральний рух у мережі, запроваджуючи суворі політики доступу, прив'язані до ідентифікаційних даних. [8]

2. Динамічне забезпечення політик. Динамічне забезпечення політик коригує заходи безпеки в реальному часі на основі поведінки користувача, стану пристрою та інших контекстуальних даних. Це дозволяє політикам змінюватися в міру зміни середовища мережі, роблячи систему адаптивною та чутливою до загроз.[9].

3. Мікросегментація на основі робочих навантажень. Ця стратегія ізолює робочі навантаження, призначаючи кожному навантаженню певні політики, що дозволяє здійснювати детальний контроль мережевого трафіку. Сегментація робочих навантажень особливо корисна в хмарних середовищах, де робочі навантаження є динамічними та можуть переміщатися між різними серверами або хмарними середовищами. [10].

4. Політика білого списку та заборона за замовчуванням. У цій стратегії весь трафік блокується, якщо він не дозволений явним чином (включений до білого списку). Це гарантує, що лише схвалені комунікації можуть відбуватися в кожному мікросегменті. Така позитивна модель безпеки забезпечує відмову в обробці невизнаного трафіку, що значно зменшує поверхню атаки. [11].

5. Інтеграція з програмно-визначеними мережами (SDN). SDN дозволяє програмно визначати політики, які контролюють трафік між сегментами. Ця інтеграція забезпечує гнучкість і масштабованість, особливо в хмарних і віртуалізованих середовищах. Політики можуть динамічно адаптуватися відповідно до зміни топології мережі.[12]

6. Сегментація на рівні периферії. Для промислових кіберфізичних систем (ICPS) і розподілених середовищ сегментація на рівні периферії ізолює мікросервіси та пристрої на межі мережі, забезпечуючи додатковий захист для систем, що працюють за межами традиційних центрів обробки даних.[13].

Одним з ключових аспектів при проектуванні мікросегментації в архітектурі Нульової Довіри є визначення оптимального рівня гранулярності. Дрібнозерниста сегментація, де кожне робоче навантаження, користувач або пристрій ізольовані, забезпечує вищий рівень безпеки шляхом мінімізації поверхні атаки. Проте, дрібнозерниста сегментація збільшує складність і може вплинути на продуктивність мережі.

Для проектування мікросегментації мережі в корпоративній інфраструктурі необхідно обзавестися розумінням та баченням з яких компонентів та елементів вона складається. Все що було в межах периметра безпеки однорангової мережі і якось собі співісновало та комунікувало між собою повинно бути ідентифіковане та прокласифіковане. На даному етапі доцільним буде використання документації та знань зібраних при аналізі корпоративної інфраструктури на етапі оцінки мережі як частини міграції до архітектури Нульової довіри. [14]

Проектування мікросегментації передбачає подальше застосування політик безпеки та організації контролю доступу між сегментами. Цілями такого дійства є запобігання несанкціонованого доступу до чутливих даних а також локалізація та ізоляція скомпрометованого сегменту та мінімізація горизонтального руху зловмисників до інших компонентів корпоративної інфраструктури та їх потенційної компрометації. Не дивлячись на очевидну безпекову цінність реалізація щільної мікросегментації має наступні недоліки:

© Сиротинський Р. М., Тишик І. Я. (2025). Особливості проектування мікросегментації мережі при побудові архітектури нульової довіри. Сучасний захист інформації, 1(61), 229–240. https://doi.org/10.31673/2409-7292.2025.012325.

- вартість реалізації напряму залежить від кількості зон файрволу та точок застосування політик безпеки, що при щільній мікросегментації може спричинити перевищення виділеного бюджету на впровадження
- Складність управління та операційної підтримки суттєво підвищується
- збільшення точок контролю доступу на шляху проходження трафіку впливає на пропускну здатність мережевої інфраструктури та підвищує затримку що може знизити її показники продуктивності нижче допустимого рівня
- велика кількість політик безпеки підвищує операційне навантаження на їх підтримку та впровадження
- високодинамічні середовища можуть бути погано сумісними з умовами експлуатації корпоративної інфраструктури при щільній мікросегментації

Таким чином кількість та структура сегментів в мережі повинна бути оптимальною щоб з однієї сторони виконувати поставлені безпекові завдання, а з іншої не погіршувати продуктивність та керованість мережі і залишатися в рамках виділеного бюджету на реалізацію.

Можна по різному підходити до сегментації мережі. Пропонується комплексний підхід на основі категоризації активів за певними ключовими ознаками. Оскільки кількість ознак на конкретний актив буде варіюватися - доцільним буде використання тегів чи позначок для подальшого аналізу та планування сегментації.

Базовим може бути наступний набір ознак мережевих активів:

- функціональна роль
- приналежність до певного корпоративного сервісу
- рівень чутливості даних хоста або критичність самого хоста
- ймовірність компрометації
- розташування в мережі

Протегувавши ассети мережі доцільним буде провести їх класифікацію та групування по рівнях.

Уточнення корпоративних систем за рівнями передбачає організацію системних компонентів або структур у окремі ієрархічні рівні, кожен з яких має певні ролі та обов’язки. Цей багаторівневий підхід зазвичай застосовується в таких сферах, як управління, інформаційні системи та структури управління, щоб спростити складність і підвищити ефективність. Рівні — це ієрархічні рівні в системі, кожен з яких призначений для виконання певних завдань або функцій. У корпоративних системах вони можуть включати операційний, управлінський і стратегічний рівні для ефективного розподілу відповідальності.[15]

Рівневість спрощує складні системи, розділяючи їх на керовані рівні, покращує прийняття рішень шляхом уточнення ролей і покращує адаптивність шляхом ізоляції змін на певних рівнях [16]. На основі функції та критичності хоста проводиться поділ всіх ассетів на рівні наступним чином:

- Рівень 1 - Критичні системи;
- Рівень 2 - Важливі системи;
- Рівень 3 - Загальні системи.

Розуміючи рівень всіх корпоративних хостів, та беручи до уваги їхні ознаки - наступним кроком буде розроблення стратегії сегментації мережі та планування точок контролю доступу. В даному випадку на прийняття кінцевого рішення можуть впливати лімітації на створення мережевих зон у файрволів на базі яких буде відбуватися сегрегація, проте не варто брати їх до уваги при первинному проектуванні, а залишити на етап оптимізації при потребі.

В залежності від рівня систем та їх типу і розміщення пропонується використовувати наступні зони корпоративного файрволу:

- зона обмеженого доступу для систем рівня 1;
- захищена зона для систем рівня 2;

© Сиротинський Р. М., Тишик І. Я. (2025). Особливості проектування мікросегментації мережі при побудові архітектури нульової довіри. Сучасний захист інформації, 1(61), 229–240. https://doi.org/10.31673/2409-7292.2025.012325.

- публічна зона для систем рівня 3 які повинні бути доступними з інтернету;
- користувацька зона для корпоративних робочих станцій;
- сервісна зона для транзитних сегментів мережі.

З точки зору конфігурації зони на файрволі різниці ніякої між ними немає, проте таким чином закладається розуміння рівня захищеності конкретної зони в майбутньому засобами контролю доступу файрвола та дає можливість більш чітко уявляти призначення зони що буде корисно при розподілі всіх корпоративних хостів по відповідних сегментах мережі. В залежності від рівня системи, приналежності до сервісу та розміщення в мережі - хост може бути поміщений в індивідуальний сегмент або груповий. В свою чергу групові сегменти мережі що обслуговуються однією зоною можуть містити якусь кількість хостів згрупованих за певною ознакою та з урахуванням їх рівня.

Таким чином традиційна мережева топологія що складається з 2-3 зон файрвола та 2-3 сегментів мережі повинна перетворитися в багатосегментну топологію з використанням відповідної кількості зон файрвола для забезпечення мікросегментації мережі - що і є ціллю при побудові архітектури нульової довіри.

Проте кількість сегментів мережі зазвичай не може відповідати кількості хостів в корпоративній мережі з огляду на обмежувальні фактори. До таких належать обмеження на кількість зон файрвола, зниження пропускної здатності та підвищення затримки при послідовному проходженні декількох файрволів а також операційна складність первинного впровадження політик контролю доступу та їх ефективної операційної підтримки. Отже, маючи певний скінченний ресурс для забезпечення сегментування мережі слід розробити оптимальний підхід з поділу всього парку корпоративних хостів на відповідні сегменти з подальшою розробкою політик безпеки між ними.

Вплив на проектування мікросегментації будуть мати декілька ключових факторів які формуватимуть вимоги та обмеження до розроблювальної топології, наприклад:

- підвищення стійкості мікросегментованої мережі до кіберзагроз та горизонтального переміщення
- мінімально допустимий рівень продуктивності мережі
- сегментація не перешкоджає чинним бізнес операціям
- витрати на впровадження мікросегментації не перевищують певний бюджет

Оскільки мікросегментація є частиною архітектури нульової довіри – а це перш за все про підвищення рівня захищеності корпоративної інфраструктури – ключовим фактором буде забезпечення стійкості до кіберзагроз та мінімізація горизонтального переміщення. З його забезпечення варто почати а вже по тому оптимізовувати під інші вимоги.

Так як кількість мікросегментів мережі майже напевно не буде відповідати кількості хостів в мережі - очевидним є те що на 1 мікросегмент буде припадати якась кількість хостів які будуть в ньому розміщені. Чи робити всі мікросегменти одинакової ємності з точки зору розміщених в них хостів – такий підхід не буде мати якоїсь очевидної переваги, а ось недоліки будуть присутніми. Отже гранулярність мікросегментів буде неоднорідною, і це має зміст, враховуючи попередній поділ корпоративних хостів на рівні та різне їх розміщення в мережі. Якісь хости будуть розміщені в індивідуальних сегментах, якісь будуть згруповані за певною ознакою і розміщені в спільному сегменті, з різною щільністю.

Належна гранулярність мікросегментації забезпечує захист кожного сегмента, підтримуючи низьку затримку та мінімальне операційне навантаження. Надмірно деталізована сегментація може призводити до зниження продуктивності, тоді як надто загальна гранулярність може неефективно обмежувати загрози [17].

Ефективна гранулярність гарантує, що заходи безпеки не потребують надмірних ресурсів, які могли б підвищити операційну складність і витрати. Добре збалансований підхід забезпечує належний рівень безпеки, зберігаючи ефективність системи [18].

© Сиротинський Р. М., Тишик І. Я. (2025). Особливості проектування мікросегментації мережі при побудові архітектури нульової довіри. Сучасний захист інформації, 1(61), 229–240. https://doi.org/10.31673/2409-7292.2025.012325.

Корпоративні вузли, які вважаються найкритичнішими в інфраструктурі з огляду на їхню роль чи рівень даних якими вони оперують потребуватимуть найретельнішого контролю доступу і щоб його забезпечити слід виключити неконтрольовані підключення від інших, потенційно скомпрометованих вузлів. Щоб цього досягти - такі хости повинні знаходитися в ізольованих сегментах мережі розміщених під контролем індивідуальної зони файрволу. Вартість мікросегментації 1 до 1 є найвищою, такий підхід має зміст лише з найважливішими вузлами за умови наявності достатнього файрвольного ресурсу.

Системами які варто захищати максимально ефективним способом будуть всі хости з рівнем критичності 1, до таких можна віднести наступні вузли корпоративної інфраструктури:

- Домен контролери та сервери аутентифікації
- Сервери баз даних які зберігають дані високого рівня конфіденційності
- Сервери які забезпечують ключову функцію бізнесу
- Адміністративні сервери та сервери управління

Оскільки висока гранулярність мікросегментації попри високий рівень захищеності має очевидні неминучі недоліки - всі хости мережі так розміщати недоцільно, а значить всі інші вузли повинні бути згруповані та розміщені анклавами в мікросегменти.

До середнього рівня гранулярності мікросегментів можна відносити потребу розміщення в них хостів мережі які мають певні спільні ознаки, це можуть бути сервери які є частиною одного сервісу або мають хости які виконують однакову роль в інфраструктурі. Такі хости є зміст об'єднувати та розміщати в спільний сегмент мережі під контролем єдиної зони файрволу на групу. При такому дизайні слід розуміти що компрометацію одного з хостів анклаву варто приймати як компрометацію всього сегменту, бо горизонтальне переміщення там вже не регулюється мережевим файрволом. Ймовірність компрометації також зростає, оскільки більше хостів, більше відкритих доступів на сегмент – відповідно більша площа потенційної атаки.

Даний підхід анклавного розміщення хостів в мікросегменті також може бути виправданим для високо інтегрованих сервісів які потребують або динамічного контролю доступу між вузлами, або мають високу інтенсивність обміну даними між вузлами що може нести додаткове навантаження на мережевий чи аплікаційний фаєрволи. Надлишковість в таких системах можна реалізовувати методом розділення сервісу на декілька еквівалентних робочих груп з розрахунком що при компрометації буде виведена з ладу одна група (один мікросегмент) а сусідня буде працювати незалежно.

Мікросегментація з середньою гранулярністю яка передбачає декілька хостів на один мережевий сегмент є популярним та ефективним підходом. При зваженому дизайні мікросегментів рівень безпеки все ще знаходиться на високому рівні, а кількість необхідних зон файрволу для забезпечення мікросегментації скорочується суттєво в порівнянні з підходом 1 до 1. І це суттєво впливає на собівартість рішення, яка знижується до реалістичних сум на впровадження та операційну підтримку, а також значно збільшує кількість компаній які собі можуть дозволити якісну мікросегментацію.

Для прикладу, згідно з дослідженням N. Sytnik, M. Kravchenko · 2021 середньостатистична інфраструктура середнього бізнесу може складатися з 50-250 серверів,[19] нехай середнє значення – 150. Мінімальна вартість зони корпоративного файрволу , на прикладу найдоступнішої моделі PaloAlto PA-1410 з ліцензією Threat Prevention на 3 роки складає +- 100 доларів. А отже мінімальна вартість забезпечення зонами файрволу лише для мікросегментації стартує від 15 000 доларів в випадку використання продуктів компанії PaloAlto. Така інвестиція в безпеку може бути непідйомною в певних випадках та поставити під ризик весь процес побудови архітектури нульової довіри.

Стратегія сегментації корпоративної мережі та розміщення хостів які не попали в індивідуальні сегменти може полягати в наступних підходах. Оскільки компрометація хосту певного корпоративного сервісу загрожує виходом з ладу всього сервісу - можна розглядати

© Сиротинський Р. М., Тишик І. Я. (2025). Особливості проектування мікросегментації мережі при побудові архітектури нульової довіри. Сучасний захист інформації, 1(61), 229–240. https://doi.org/10.31673/2409-7292.2025.012325.

гранулярність мікросегментції до рівня сервісу або до рівня 2 сегменти на сервіс. Змістовними будуть наступні підходи поділу сервісу на окремі сегменти:

- поділ сервісу на фронтенд частини та бекенд;
- відокремлення від сервісу серверів з базами даних з міркування додаткового захисту корпоративних даних;
- рознесення тестових, розробницьких та виробничих середовищ на окремі сегменти.

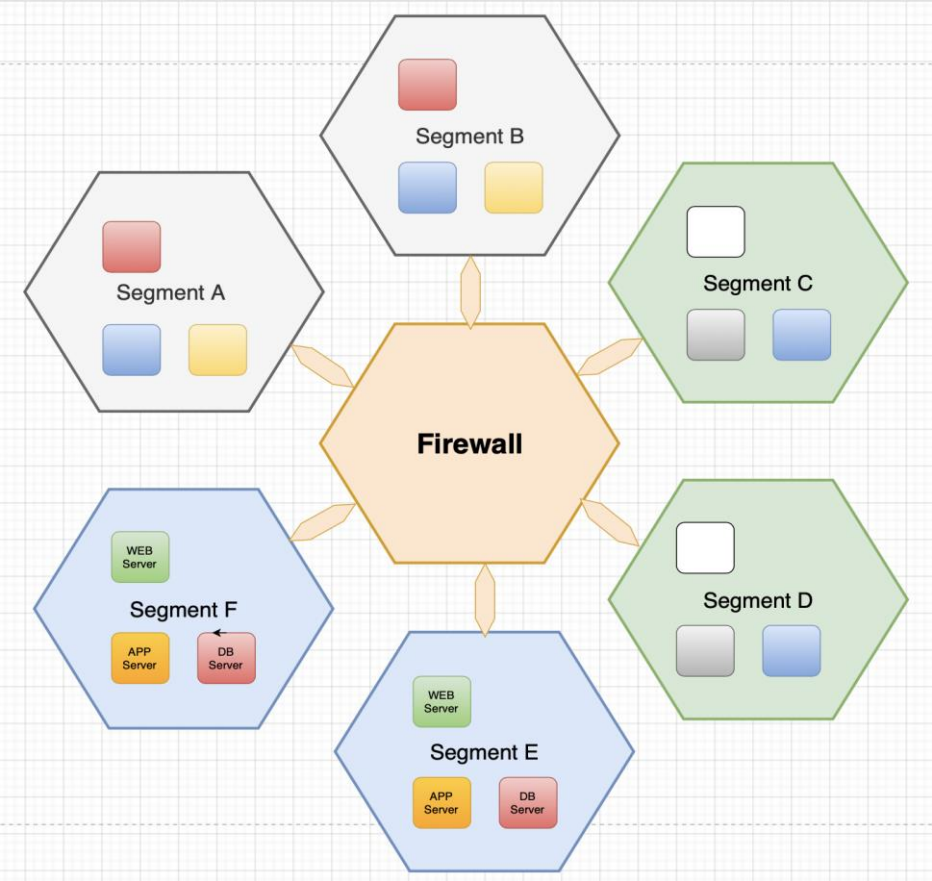

Рис.1 Надлишковість корпоративних сервісів в мікросегментах

Таким чином повний перелік хостів які підтримують корпоративні сервіси чи аплікації буде поділено на мікросегменти, що значно підсилить стійкість всієї мережі до дестабілізаційних подій методом локалізації та недопущення горизонтального руху зловмисників. Тим не менше, в корпоративній інфраструктурі залишиться ще значна кількість хостів, які є присутніми і не потребують класичної дрібної чи середньої мікросегментації, для них буде достатньо розділити їх за типом та застосувати інші підходи до обмеження трафіку.

Наприклад, пристрої, які потребують однакового рівня аутентифікації та авторизації, такі як робочі станції співробітників одного підрозділу, можуть бути згруповані. Це полегшує дотримання політики та спрощує реалізацію принципів нульової довіри.[20] Також – IoT-пристрої з обмеженою функціональністю та подібними вразливостями можуть бути згруповані в один сегмент, захищений міжмережевими екранами або сучасними рішеннями безпеки [21].

Отже до таких пристроїв можуть відноситися такі групи мережевих хостів:

- корпоративні робочі станції;
- корпоративні пристрої IoT;
- гостьові пристрої;
- сегмент підключення VPN клієнтів.

При технічній можливості можна реалізувати обмеження трафіку peer-to-peer засобами керування безпровідними мережами або списками доступу на портах комутаторів. Це альтернативні заходи які забезпечують часткову мікросегментацію в користувацьких динамічних середовищах, оскільки обмежують лише горизонтальний рух. В окрему категорію вузлів мережі які потребуватимуть особливої уваги попадають хости які знаходяться в демілітаризованій зоні або публічно опубліковані в інтернет.

Такі активи мають суттєво вищий ризик компрометації оскільки вони не захищені повністю корпоративним файрволом та мають дозволений вхідний доступ в силу архітектури сервісу до якої належать. Такі хости доступні для сканування зловмисниками 24x7 і не завжди можуть бути захищені засобами WAF. В незалежності якої критичності є дані хости, чи приналежності до якогось сервісу – важливо розміщати їх в індивідуальні сегменти та особливо прискіпливо дотримуватися принципу найменших привілеїв в усіх можливих напрямках, включаючи контроль доступу не лише до сусідніх ДМЗ хостів чи всередину мережі а й в інтернет. Доступ в обі сторони важливо дозволяти по чітко вказаних IP-адресах джерела, призначення, портах та аплікаціях.

Побутує також думка що гранулярність має динамічно адаптуватися до конкретних умов, таких як час, поведінка користувача та рівень загроз, забезпечуючи максимальну гнучкість при збереженні безпеки.[22] Це цікавий та перспективний підхід, але в даному дослідженні такі експерименти та дослідження не проводилися.

Результати досліджень

Методологію адаптивного проектування мікросегментації корпоративної мережі пропонується вдосконалити аналітичним методом на базі модифікованої подвійної матриці ризиків - див. рисунок 3. Даний метод рекомендуватиме відповідний розмір мікросегмента для розміщення в ньому хоста чи хостів мережі в залежності від критичності хоста з точки критичності хоста з точки зору впливу на бізнес чи рівня конфіденційності даних по осі Y та ризик фактору хоста по осі X який в свою чергу визначатиметься ще однією матрицею ризиків на основі розміщення хоста в корпоративній мережі по осі Y та рівнем схильності до компрометації в залежності від безпекових факторів по осі X.

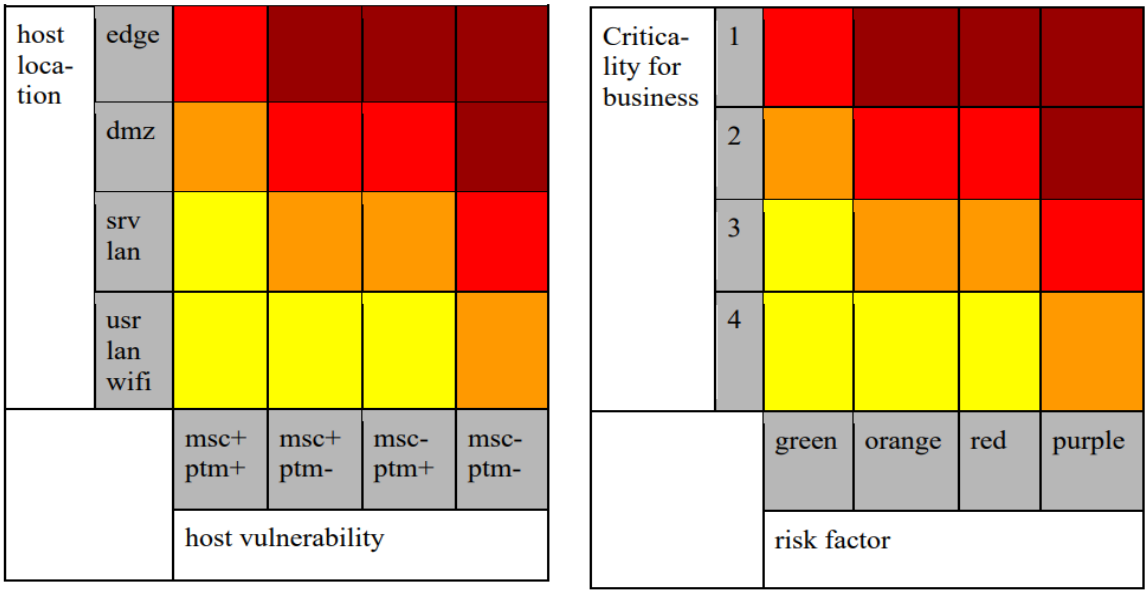

Рис 2. Матриці вразливості хоста зліва та розміру мікросегмента зправа

Такими факторами номінально можуть бути покриття процесом керування виправленнями (ptm) та можливість конфігурації параметрів безпеки та підтримка встановлення безпекових додатків (msc). Таким чином провівши аналіз безпекових факторів та співставивши результати з ступенем критичності хоста можемо розрахувати вимогу до

© Сиротинський Р. М., Тишик І. Я. (2025). Особливості проектування мікросегментації мережі при побудові архітектури нульової довіри. Сучасний захист інформації, 1(61), 229–240. https://doi.org/10.31673/2409-7292.2025.012325.

гранулярності мікросегментації для кожного з мережевих хостів в наступних співвідношеннях колір-сегмент:

- Пурпурний колір – індивідуальний мікросегмент
- Червоний колір – мікросегмент з хостами які належать до одного сервісу без критичних для бізнесу аплікацій чи сховищ з даними високого рівня чутливості. Такі хости розміщуються в окремому мікросегменті, поділяючи середовище корпоративного сервісу на декілька розділених середовищ
- Оранжевий колір – мікросегмент з будь якими хостами які належать до одного корпоративного сервісу
- Жовтий колір – мікросегмент з хостами які належать до різних сервісів або сегмент мережі в якому контроль горизонтального переміщення забезпечується списками контролю доступу або функціями блокування peer-to-peer з'єднань

Даний підхід заслуговує на увагу як інструмент ітераційного проектування мікросегментації корпоративної мережі та не претендує на звання універсального і безальтернативного підходу. Специфіка кожної окремої інфраструктури повинна братися до уваги і вносити свої корективи в процес проектування.

Після проведеного аналізу та проектування мікросегментації корпоративна мережева інфраструктура набуває вигляду певної сукупності мікросегментів різної ємності які об'єднані між собою проте доступ регулюється політиками безпеки файрвола. Для забезпечення первинної цінності мікросегментації - кожен мікросегмент повинен бути забезпеченим окремою зоною корпоративного файрволу, що в подальшому дасть можливість здійснювати контроль доступу в усіх напрямках та унеможливити чи суттєво мінімізовувати горизонтальне переміщення. Окремо варто згадати за різного роду службові зони, такі як зони що відповідають за зв'язність файрволів між собою, а також зони інтерфейсів які виступають точками приєднання до інших мережевих пристроїв, наприклад роутери чи ВПН концентратори. Для ефективного та гранулярного контролю доступу зони для таких сегментів повинні бути різні.

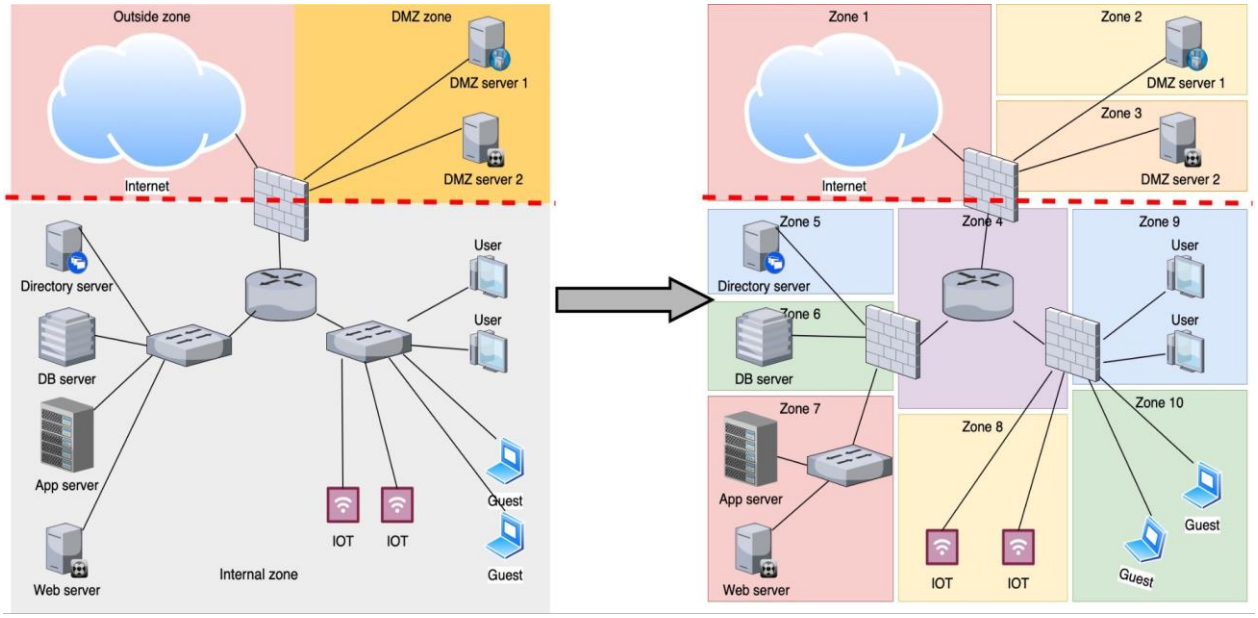

Рис. 3 Ілюстративний приклад мікросегментації корпоративної інфраструктури

Як приклад розглянемо проектування мікросегментації для невеликої корпоративної мережі яка складається з 6-7 серверів та парку користувацьких пристроїв 3 різних шаблонів. Реалізація даної моделі вимагатиме збільшення файрволів з 1 до 2-3 пристроїв та збільшення зон файрвола з 3 до 10.

Даний приклад розроблення мікросегментації відображає зміну архітектури мережі для забезпечення гнучкого контролю доступу між її компонентами та демонструє зростання вартості реалізації в порівнянні з одноранговою мережею від одного файрволу на 3 зони до 2-3 файрволів з підтримкою 16 зон сумарно (10 по факту, 6 - для розширення).

Реалізація мікросегментації на мережевому рівні це завжди підвищення складності мережевої топології, збільшення кількості політик безпеки в майбутньому та вимога додаткових фаєрволів чи ресурсів мережевого фаєрвола. Розмір корпоративної інфраструктури значною мірою впливає на кількість необхідних зон файрволів для забезпечення мікросегментації та меншою мірою впливає на необхідну кількість файрволів для забезпечення контролю трафіку в різних місцях. Проте в любому випадку це призводить до зростання вартості реалізації мікросегментації та підвищення витрат на операційну підтримку в порівнянням з витратами на малосегментовані мережі.

В випадку якщо спроектований дизайн мікросегментації вимагає кількість фаєрволів та їхніх зон яка перевищує закладений бюджет на реалізацію - розроблений дизайн може переглядатися на предмет оптимізації та зменшення необхідних ресурсів контролю мережевого трафіку або пошуку інших засобів реалізації мікросегментації. Шляхи оптимізації можуть включати перегляд критичності корпоративних хостів з застосуванням матриці ризиків для визначення рівня впливу на бізнес та інфраструктуру в разі їхньої компрометації. Хости які чинять менший вплив на бізнес процеси компанії або мають менший потенціал при компрометації можна обєднювати в спільні мікросегменти і таким чином знижувати загальну кількість необхідних файрволів, їх зон та кількість політик які треба створити а потім підтримувати.

Серед сучасних методів оптимізації мікросегментації відноситься впровадження динамічних правил, які адаптуються до поведінки користувачів і трафіку, зменшуючи потребу в статичних, ресурсомістких конфігураціях. Це дозволяє зменшити кількість активних зон при збереженні гнучкості.[23]

Щодо інших підходів реалізації мікросегментації - до таких можна віднести прийоми обмеження горизонтального трафіку для користувацьких підключень в динамічних сегментах корпоративних мереж. Контроль доступу до інших ресурсів мережі є частковим і здебільшого статичним. Горизонтальний трафік блокується засобами організації безпровідних мереж, а у випадку дротових підключень з застосуванням списків доступу до портів на комутаторі. Вертикальний доступ може бути дозволений або ні, в останньому випадку передбачається підключення ВПН з автентифікацією та авторизацією для отримання вертикального доступу до корпоративних ресурсів або інтернету. Таким чином кожен користувач як клієнт мережі є відділеним від інших однорангових клієнтів горизонтально а його вертикальний доступ регулюється. Така практика є виправданою в силу динамічності середовища, уніфікації контролю доступу та здешевлення реалізації.

Висновки

Встановлено, що Мікросегментація є важливим елементом архітектури нульової довіри, оскільки вона поділяє мережу на ізольовані сегменти, запобігаючи бічному руху атакувальників у межах корпоративної мережі організації. Процес впровадження мікросегментації передбачає попередній аналіз особливостей корпоративної інфраструктури організації, врахування яких дозволяє розробити її оптимальний дизайн. Щільна мікросегментація суттєво підвищує захищеність інфраструктури проте є складною в реалізації та дороговартісною. Індивідуальне проектування мікросегментації на базі аналізу існуючої інфраструктури, розташування її вузлів та оцінки рівня критичності для бізнесу дає можливість скоротити витрати на реалізацію та подальше її обслуговування, забезпечуючи при цьому відповідність принципам нульової довіри.

В роботі охарактеризовано особливості проектування мікросегментації, проаналізовано її вплив на рівень безпеки, функціонування та керованість елементів корпоративної

© Сиротинський Р. М., Тишик І. Я. (2025). Особливості проектування мікросегментації мережі при побудові архітектури нульової довіри. Сучасний захист інформації, 1(61), 229–240. https://doi.org/10.31673/2409-7292.2025.012325.

інфраструктури, досліджено вплив на інфраструктуру впровадження мікросегментації з різною гранулярністю. Запропонований аналітичний метод адаптивного проектування мікросегментації корпоративної мережі з використанням подвійної матриці ризиків для аналізу хостів та визначення оптимального рівня гранулярності мікросегментів в залежності від певних факторів. Встановлено, що не дивлячись на високий рівень захисту при мікросегментації з індивідуальними сегментами для всіх хостів мережі, - оптимальним рішенням є застосування дизайну мікросегментації з варіативним розміром мікросегментів в залежності від критичності хоста, його безпекового статусу та розташування.

Подальшими напрямами досліджень можуть бути поєднання ефективного впровадження з операційними підтримками політик безпеки в мікросегментованій мережі як елемент побудови архітектури нульової довіри.

Перелік посилань

1. Ma, M., Yu, Z., & Liu, B. (2023). Automatic Generation of Network Micro-Segmentation Policies for Cloud Environments. 2023 4th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT), 1-5. https://doi.org/10.1109/AINIT59027.2023.10212857.

2. Basta, N., Ikram, M., Kâafar, M., & Walker, A. (2021). Towards a Zero-Trust Micro-segmentation Network Security Strategy: An Evaluation Framework. NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium, 1-7. https://doi.org/10.1109/NOMS54207.2022.9789888.

3. Noel, S., Swarup, V., & Johnsgard, K. (2021). Optimizing network microsegmentation policy for cyber resilience. The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, 20, 57 - 79. https://doi.org/10.1177/15485129211051386.

4. Mujib, M., & Sari, R. (2020). Performance Evaluation of Data Center Network with Network Micro-segmentation. 2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE), 27-32. https://doi.org/10.1109/ICITEE49829.2020.9271749.

5. Liu, Y., Liu, G., Du, H., Niyato, D., Kang, J., Xiong, Z., Kim, D., & Shen, X. (2024). Hierarchical Micro-Segmentations for Zero-Trust Services via Large Language Model (LLM)-enhanced Graph Diffusion. ArXiv, abs/2406.13964. https://doi.org/10.48550/arXiv.2406.13964.

6. Mujib, M., & Sari, R. (2020). Performance Evaluation of Data Center Network with Network Micro-segmentation. 2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE), 27-32. https://doi.org/10.1109/ICITEE49829.2020.9271749.

7. Sheikh, N., Pawar, M., & Lawrence, V. (2021). Zero trust using Network Micro Segmentation. IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 1-6. https://doi.org/10.1109/INFOCOMWKSHPS51825.2021.9484645.

8. Keeriyattil, S. (2019). Microsegmentation and Zero Trust: Introduction. Zero Trust Networks with VMware NSX. https://doi.org/10.1007/978-1-4842-5431-8_2.

9. Zhang, P., Tian, C., Shang, T., Liu, L., Li, L., Wang, W., & Zhao, Y. (2021). Dynamic access control technology based on zero-trust light verification network model. 2021 International Conference on Communications, Information System and Computer Engineering (CISCE), 712-715. https://doi.org/10.1109/CISCE52179.2021.9445896.

10. Sheikh, N., Pawar, M., & Lawrence, V. (2021). Zero trust using Network Micro Segmentation. IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 1-6. https://doi.org/10.1109/INFOCOMWKSHPS51825.2021.9484645.

11. Keeriyattil, S. (2019). Microsegmentation and Zero Trust: Introduction. Zero Trust Networks with VMware NSX. https://doi.org/10.1007/978-1-4842-5431-8_2.

12. Paul, B., & Rao, M. (2022). Zero-Trust Model for Smart Manufacturing Industry. Applied Sciences. https://doi.org/10.3390/app13010221.

13. Lei, W., Pang, Z., Wen, H., Hou, W., & Zhang, X. (2023). Edge-enabled Zero Trust Architecture for ICPS with Spatial and Temporal Granularity. 2023 IEEE 6th International Conference on Industrial Cyber-Physical Systems (ICPS), 1-6. https://doi.org/10.1109/ICPS58381.2023.10127999.

14. Syrotynskyi, R., Tyshyk, I., Kochan, O., Sokolov, V., Skladannyi, P. (2024). Methodology of network infrastructure analysis as part of migration to zero-trust architecture (short paper). CSDP-2024: Cyber Security and Data Protection, June 30, 2024, Lviv, Ukraine, 97-105.

15. Douma, S. (1997). The two-tier system of corporate governance. Long Range Planning, 30, 612-614. https://doi.org/10.1016/S0024-6301(97)00047-2.

16. Dowling, N., Punt, A., Little, L., Dichmont, C., Smith, D., Haddon, M., Sporcic, M., Fulton, E., & Gorton, R. (2016). Assessing a multilevel tier system: The role and implications of data quality and availability. Fisheries Research, 183, 588-593. https://doi.org/10.1016/J.FISHRES.2016.05.001.

17. Mujib, M., & Sari, R. (2020). Performance Evaluation of Data Center Network with Network Micro-segmentation. 2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE), 27-32. https://doi.org/10.1109/ICITEE49829.2020.9271749.

18. Khan, M. (2023). Zero trust architecture: Redefining network security paradigms in the digital age. World Journal of Advanced Research and Reviews. https://doi.org/10.30574/wjarr.2023.19.3.1785.

19. Sytnik, N., & Kravchenko, M. (2021). Application of knowledge management tools: Comparative analysis of small, medium, and large enterprises. Journal of Entrepreneurship, Management and Innovation. https://doi.org/10.7341/20211745.

20. Keeriyattil, S. (2019). Microsegmentation and Zero Trust: Introduction. Zero Trust Networks with VMware NSX. https://doi.org/10.1007/978-1-4842-5431-8_2.

21. Da Rocha, B., De Melo, L., & De Sousa, R. (2021). Preventing APT attacks on LAN networks with connected IoT devices using a zero-trust based security model. 2021 Workshop on Communication Networks and Power Systems (WCNPS), 1-6. https://doi.org/10.1109/WCNPS53648.2021.9626270.

22. Wenxin Lei et al. "Edge-enabled Zero Trust Architecture for ICPS with Spatial and Temporal Granularity." 2023 IEEE 6th International Conference on Industrial Cyber-Physical Systems (ICPS) (2023): 1-6. https://doi.org/10.1109/ICPS58381.2023.10127999.

23. S. Noel et al. "Optimizing network microsegmentation policy for cyber resilience." The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, 20 (2021): 57 - 79. https://doi.org/10.1177/ 1548512-9211051386.

Надійшла 19.02.2025