УДК 004.056.53:65.012.8 **DOI:** 10.31673/2412-9070.2024.030711
О. Б. ПРИДИБАЙЛО[1], ст. викладач, здобувач, ORCID: 0009-0003-7967-5827,
Р. В. ПРИДИБАЙЛО[1], аспірант, ORCID: 0009-0003-1747-7518,
В. О. ЯСКЕВИЧ[2], доцент, ORCID: 0000-0002-5796-2521,
Ю. В. ЯСКЕВИЧ[2], аспірант, ORCID: 0009-0005-6084-5229,
[1] Державний університет інформаційно-комунікаційних технологій, Київ
[2] Київський столичний університет імені Бориса Грінченка

АРХІТЕКТУРА НУЛЬОВОЇ ДОВІРИ: ЛОГІЧНІ КОМПОНЕНТИ ТА ПІДХОДИ ЗАПРОВАДЖЕННЯ

Архітектура нульової довіри (АНД) — це сучасний підхід до кібербезпеки, який іде на зміну традиційній моделі безпеки на основі периметра. У моделі нульової довіри організації не автоматично довіряють жодному користувачеві або пристрою, незалежно від того, чи вони перебувають всередині чи поза корпоративною мережею. Замість цього вона передбачає, що загрози можуть виникнути як з боку внутрішніх, так і зовнішніх джерел, і перевіряє кожного користувача та пристрій, котрі намагаються отримати доступ до ресурсів.

Основні принципи цього напрямку розвитку програмного забезпечення:

• перевірка ідентичності: людям потрібно підтверджувати свою ідентичність перед отриманням доступу до ресурсів. Це часто передбачає багаторівневу автентифікацію та надійні методи верифікації;

• доступ із найменшими привілеями: користувачам надається найменший доступ, потрібний для виконання їх завдань. Доступ обмежується лише до істотних речей, зменшуючи потенційний вплив порушення безпеки;

• мікросегментація: передбачає сегментування мережі на дрібному рівні, що дає змогу ізолювати та захищати окремі ресурси;

• шифрування даних: шифрування застосовується як у процесі передавання, так і у спокої, щоб захистити дані від несанкціонованого доступу;

• відсутність прихованої довіри, застосування принципу «ніколи не довіряй, завжди перевіряй» означає, що перевірка потрібна на кожному етапі доступу.

У статті розглянуто сучасні виклики та підходи до забезпечення кібербезпеки за умов швидкого розвитку хмарних технологій. Зокрема, проаналізовано зсув у використанні контейнерів у розгортанні програмного забезпечення та його вплив на модель кібербезпеки. Підходи до безпеки, що базуються на концепції АНД, висвітлено в контексті нових вимог та можливостей.

Детально описано ключові логічні компоненти АНД, зокрема механізм політики та адміністратор політики, і зазначено їхню взаємодію у створенні безпечного середовища. Також надано огляд джерел даних, використаних для створення правил політики доступу та врахування їх у механізмах АНД. Запропоновано підходи до впровадження АНД для робочих процесів у корпоративних середовищах: покращене керування ідентифікацією, логічну мікросегментацію та сегментацію на основі мережі. Кожен із цих підходів має свої переваги та беруться до уваги залежно від потреб індивідуальної організації.

Ключові слова: архітектура; кібербезпека; підприємство; безпека мережі; нульова довіра; архітектура нульової довіри; політики; механізми політик.

Вступ

Хмарні обчислення кардинально змінили підхід до розгортання та доступу до даних і послуг, підвищивши доступність, гнучкість і розвинувши модель інвестування завдяки зменшенню початкових витрат та пов'язаних із ними ризиків. Перехід до хмарних рішень став ще більш прискореним під час пандемії COVID-19. Прагнучи до стійкості та гнучкого попиту на обчислювальну потужність і діяльність більш, ніж будь-коли, перекочувала в онлайн-простір.

Навіть віртуалізований підхід до розгортання, створений на основі віртуальних машин, кращий з погляду використання ресурсів і масштабованості порівняно з традиційним розгортанням, реалізованим за допомогою фізичних серверів із запущеними програмами, втрачає привабливість на користь ери розгортання контейнерів, заснованої на архітектурі мікросервісів. Цей зсув дає змогу рухатися до неперервного доставляння, максимальної швидкості і гнучкості розгортання. Фонд хмарних обчислень (CNCF) провів опитування, опубліковане на початку 2023 року, яке показало, що «контейнери — це нова норма».

Серед 2063 учасників опитування 44% повідомили, що використовують контейнери майже для всіх застосунків і бізнес-сегментів, а ще 35% сказали, що застосовують контейнери принаймні для кількох виробничих застосувань.

Ці тенденції створюють нові проблеми та перспективи у сфері безпеки. Підхід «замка та рову»,

заснований на забезпеченні безпеки периметра з чітким розмежуванням між внутрішньою довіреною зоною та зовнішньою ненадійною мережею, більше не застосовується в епоху деперіметралізації, в якій немає певних фізичних периметрів із розподілом даних за пристроями та кількома платформами.

Уже 2004 року завдяки групі Jericho Forum [1] стало відомо про труднощі визначення периметрів для їхнього захисту. Це поступово призводить до потреби в деперіметралізації самої безпеки, усунення концепції довірених зон та завжди до перевірки доступу та дій. Ці принципи були формалізовані у 2020 році Національним інститутом стандартів та технологій (NIST) та Національним центром передового досвіду в галузі кібербезпеки (NCCoE) у спеціальній публікації NIST 800-207 «Архітектура нульової довіри» [2].

Тому, в наш час наполегливою рекомендацією є перенесення або запровадження мережних рішень нульової довіри.

Мережний підхід із нульовою довірою зумовлює підвищення прозорості мережі та потоку трафіку, зменшення розкриття конфіденційних даних, зменшення впливу порушень, обмеження горизонтальних переміщень та загального поліпшення стану безпеки.

З погляду технологій оркестратор Kubernetes із 91% завантаження став стандартом де-факто, надаючи не тільки надійне програмне забезпечення, здатне впоратися з розгортанням мікросервісів, а й велику екосистему на користь стійкості до відмов. Модульність та розширюваність — ці характеристики дають змогу створювати поверх Kubernetes інші технології, здатні співіснувати та розширювати можливості оркестратора. Зробивши це, можна домогтися поділу завдань між Kubernetes, що відповідає за постійне забезпечення бажаного стану розгортань усередині кластера, мережним інтерфейсом контейнера (МІК), який керує низькорівневим мережним підключенням кластера та сервісною сіткою, розташованою на верхній частині МІК для керування зв'язком між службами, надаючи додаткові можливості щодо трафіку керування, безпеки та спостереження.

Будь-яке корпоративне середовище може бути спроєктовано з урахуванням принципів нульової довіри. Більшість організацій вже мають деякі елементи нульової довіри до своєї корпоративної інфраструктури або перебувають у дорозі за допомогою впровадження політик і передових практик інформаційної безпеки та стійкості.

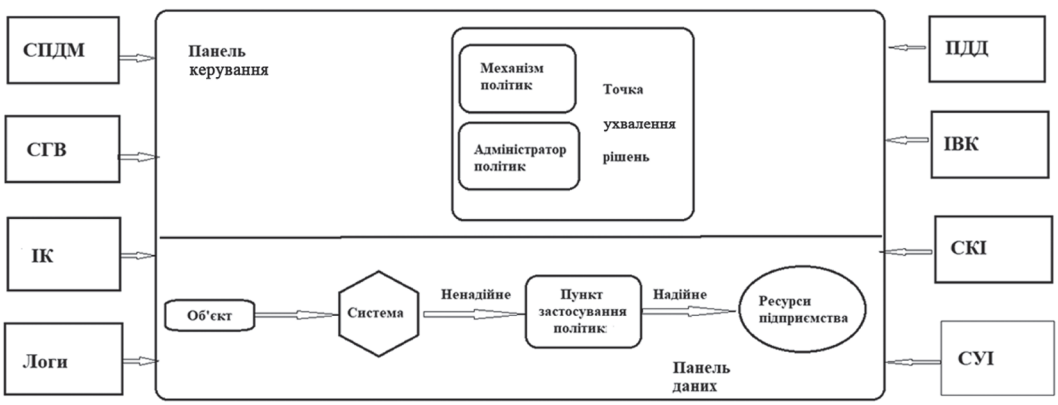
Деякі сценарії розгортання та варіанти використання легко піддаються архітектурі з нульовою довірою.

Основна частина

Для того, щоб розгорнути АНД на будь-якому підприємстві, потрібно мати достатню кількість логічних компонентів, які зможуть працювати як локально, так і через хмарні технології. Загальна схема побудови (рисунок) показує зв'язки між компонентами, а також взаємодію компонентів між собою. Точка ухвалення рішень (ТУР) або точка вибору правил в комп'ютерній мережі — зазвичай сервер, що містить політики (правила) маршрутизації й ухвалює рішення про їхній вибір для своїх клієнтів (маршрутизаторів та комутаторів). На схемі видно, що ТУР містить два логічні компоненти: механізм політик та адміністратор політик. Логічні компоненти та дані використовують різні панелі для взаємодії, керування та передавання даних.

Політика використовується для поєднання набору правил. Зазвичай набір таких правил є одним бізнес-правилом. Отже, вирішується відразу кілька завдань. По-перше, невеликі частини логічних умов, які у правилах можна легко використовувати неодноразово, без дублювання цих умов. По-друге, такий поділ на частини полегшує розуміння всього бізнес-правила та спрощує його супровід.

Політика охоплює ціль (target), правила (rules), алгоритм комбінації правил (rule-combine algorithm), зобов'язання (obligation), рекомендації (advice).



Логічні компоненти ядра НД

• Механізм правил (політик) (МП) надає доступ до ресурсу для даного об'єкта та відповідає за остаточне рішення про таке надання. МП використовує вхідні дані із зовнішніх джерел (наприклад, система CDM, служби аналізу загроз) як вхідні дані для алгоритму довіри для надання, заборони або відповіді ресурсу. МП пов'язаний з компонентом адміністратора політик. Механізм правил (політик) приймає та реєструє рішення (як ухвалене або відхилене), а адміністратор політик уже виконує надане йому рішення.

• Адміністратор політик (АП) відповідає за внутрішні правила організації, зокрема директиви, політики, робочі процедури тощо. Він відповідає за створення, оновлення, керування та поширення серед працівників директив усередині компанії, забезпечення того, щоб співробітники компанії були знайомі з директивами та розуміли їх. Також АП координує розроблення політик та інших нормативних актів, аналізує, моніторить, вимірює та постійно поліпшує політики та правила компанії.

Адміністратор політик відповідає за встановлення, закриття шляху зв'язку між суб'єктом і ресурсом. Він тісно пов'язаний із МП і покладається на його рішення остаточно дозволити або заборонити сеанс. Цей зв'язок здійснюється через панель керування.

• Пункт застосування політик (ПЗП) — це елемент системи, який запитує, а потім забезпечує виконання рішень щодо авторизації.

Це єдиний логічний компонент у АНД, але його можна розбити на два різні компоненти: клієнт (наприклад, агент на ноутбуці) і сторона ресурсу (наприклад, компонент шлюзу перед ресурсом, який контролює доступ) або один компонент порталу. За ПЗП міститься зона довіри розміщення ресурсу підприємства. На додаток до основних компонентів на підприємстві, що реалізує АНД, кілька джерел даних надають правила введення та політик, які використовуються механізмом політик під час ухвалення рішень щодо доступу. До них належать локальні джерела даних, а також зовнішні (тобто не контрольовані компанією або створені нею) джерела даних. Далі наведемо їхні складові елементи.

1. Система постійної діагностики та пом'якшення (СПДМ) призначена для збору інформації щодо поточного стану корпоративного активу та застосовує оновлення до компонентів програмного забезпечення. Корпоративна система СПДМ надає механізму політик інформацію про актив, який надсилає запит на доступ, цілісність схвалених підприємством програмних компонентів або наявність несхвалених компонентів, а також чи має актив будь-які відомі вразливості.

2. Система галузевої відповідності (СГВ) відповідає за сумісність підприємства залишатися з будь-яким регуляторним режимом, під який воно може потрапити (наприклад, закон про керування інформаційною безпекою; вимоги щодо безпеки інформації в галузі охорони здоров'я чи фінансової галузі). Це включає в себе всі правила, які підприємство розробляє для забезпечення відповідності.

3. Інформаційний(і) канал(и) (ІК) надає інформацію про загрози з внутрішніх або зовнішніх джерел, яка допомагає механізму політик ухвалювати рішення щодо доступу. Це можуть бути кілька служб, які отримують дані з внутрішніх або кількох зовнішніх джерел і надають інформацію про нещодавно виявлені атаки чи вразливості. Це також охоплює виявлені недоліки в програмному забезпеченні, виявлене зловмисне програмне забезпечення та зареєстровані атаки на інші активи, до яких механізм політики захоче заборонити доступ із корпоративних активів.

4. Журнали мережної та системної активності (логи). Ця корпоративна система збирає журнали активів, мережний трафік, дії доступу до ресурсів та інші події, які забезпечують зворотний зв'язок у режимі реального часу (або майже в реальному часі) щодо стану безпеки інформаційних систем підприємства.

5. Політики доступу до даних (ПДД). Такі набори правил можуть бути закодованими Ці політики є відправною точкою для авторизації доступу до ресурсу, оскільки вони надають основні привілеї доступу для облікових записів і програм/служб на підприємстві.

6. Інфраструктура відкритих ключів підприємства (ІВК). Ця система відповідає за створення та реєстрацію сертифікатів, виданих підприємством ресурсам, суб'єктам, службам і програмам. Також містить екосистему глобального центру сертифікації та федеральну ІВК, яка може бути або не бути інтегрованою з корпоративною ІВК.

7. Система керування ідентифікаторами (СКІ) відповідає за створення, зберігання та керування корпоративними обліковими записами користувачів і ідентифікаційними записами. Ця система містить необхідну інформацію про тему (наприклад, ім'я, адресу електронної пошти, сертифікати) та інші характеристики підприємства, такі як роль, атрибути доступу та призначені активи. Ця система часто використовує інші системи (наприклад, ІВК) для артефактів, пов'язаних з обліковими записами користувачів. Ця система може бути частиною більшої спільноти та може мати у своєму складі некорпоративних працівників або посилання на некорпоративні активи для співпраці.

8. Система керування інформацією про безпеку та подіями (СКІ) збирає інформацію, орієнтовану на безпеку, для подальшого аналізу. Потім ці дані використовуються для вдосконалення політики та

попередження про можливі атаки на активи підприємства.

Щоб запровадити архітектуру з нульовою довірою існує кілька способів. Вони відрізняються компонентами, що використовуються, і основним джерелом правил політики для організації. Кожний варіант має реалізувати всі принципи нульової довіри, але кількість компонент, які будуть використані, може різнитися. Повне рішення НД послуговуватиметься елементами трьох варіантів.

1. Покращене керування ідентифікацією. У цьому варіанті використовується ідентифікація учасників як ключовий компонент формування політик. Якщо не буде суб'єктів, які запитують доступ до підприємства ресурсів, не буде і потреби створювати політики доступу. Основна вимога на доступ до ресурсу базується на привілеях доступу, наданих даному суб'єкту. Інші такі чинники, як пристрій, що використовується, стан активів і чинники навколишнього середовища можуть змінити остаточний рівень вірогідності обчислення (і кінцевої авторизації доступу) або певним чином адаптувати результат, наприклад наданням лише часткового доступу до даного джерела даних на основі розташування в мережі.

Застосування варіанта на основі керування ідентифікацією дуже часто застосовуються з використанням моделі відкритої мережі або корпоративної мережі. Спочатку доступ до мережі надається всім особам, але доступ до корпоративних ресурсів обмежується особами з відповідними правами доступу. Таке базове підключення все ж має певний недолік: зловмисники все одно можуть намагатися досліджувати мережу та використовувати її для здійснення атак або ж проти третьої сторони. Підприємствам ще потрібно стежити і реагувати на таку поведінку, перш ніж вона вплине на робочі процеси.

Підхід, керований ідентифікацією, добре працює з моделлю ресурсного порталу, оскільки ідентифікація та статус пристрою надають вторинні дані підтримання для ухвалення рішень щодо доступу. Варіанти, що керуються ідентифікацією, також добре працюють для підприємств, які використовують хмарні програми (сервіси), котрі можуть не дозволяти використовувати компоненти безпеки НД, що належать або керуються підприємством.

2. Логічна мікросегментація. Підприємство може вибрати впровадження АНД на основі розміщення окремих осіб або груп в унікальному сегменті мережі, захищеному компонентом безпеки шлюзу. У цьому варіанті підприємство розміщує інтелектуальні комутатори (або маршрутизатори) або брандмауери наступного покоління або шлюзи спеціального призначення, які діють як ПЗП, захищаючи кожен ресурс або невелику групу пов'язаних ресурсів. Ці шлюзові пристрої динамічно надають доступ до індивідуальних запитів від клієнта, активу чи послуги. Такий підхід застосовується для різноманітних варіантів використання та моделей розгортання, оскільки захисний пристрій діє як ПЗП, а керування цими пристроями діє як компонент МП/АП.

3. Сегментація на основі мережі. Даний підхід використовує мережну інфраструктуру для реалізації АНД. Реалізацію АНД може бути досягнуто за допомогою накладеної мережі. Цей підхід, який іноді називають програмно визначеним периметром, прийнятний і часто охоплює концепції програмно-визначених мереж і мереж на основі намірів. У цьому підході МП виступає як мережний контролер, який налаштовує та переконфігуровує мережу на основі рішень, ухвалених АП. Клієнти продовжують запитувати доступ через ПЗП, якими керує компонент АП. Коли підхід реалізовано на мережному рівні застосунків, найбільш загальною моделлю розгортання є агент/шлюз.

Висновки

Перехід до хмарних обчислень та використання контейнерів призводить до зростання можливих загроз безпеки даних та потреби в архітектурі нульової довіри.

Архітектура нульової довіри передбачає принцип «ніколи не довіряй, завжди перевіряй», що дає змогу створити ефективну систему контролю доступу та керування безпекою в сучасному корпоративному середовищі.

Існує кілька практичних підходів до впровадження архітектури нульової довіри, серед яких покращене керування ідентифікацією, логічна мікросегментація та сегментація на основі мережі.

Компанії можуть адаптувати модель архітектури нульової довіри під свої специфічні потреби та середовище. Це підвищує ефективність, стійкість до відмов і допомагає зменшити ризики.

На додаток, упровадження такої архітектури може бути розглянуто як частина стратегії дотримання регулятивних вимог і підвищення рівня корпоративної безпеки.

Незважаючи на потенційні виклики, архітектура нульової довіри є ключовим чинником у забезпеченні гнучкості та безпеки в контексті цифрової трансформації та швидшої її реалізації.

Список використаної літератури

*1. **Van Cleeff A., Wieringa R. J.** Rethinking de-perimeterisation: Problem analysis and solutions // IADIS International Conference Information Systems 2009. Barcelona (ES), 2009. P. 105–112.*

*2. **Zero** trust architecture / S. W. Rose, O. Borchert, S. Mitchell, S. Connelly. August, 2020.*

3. ***Liu Q.*** *Data center security protection in the industry based on zero-trust architecture // Security & Informatization. 2018. № 12. P. 107–109.*

4. ***Yang Z., Jin M., Zhang X.*** *Research on Security Technology of Zero Trust in Cloud Business // Information Security and Communications Privacy. 2020. № 3. P. 91–98.*

5. ***Zuo Y.*** *Zero-trust architecture: a new paradigm for network security. Financial Computerizing. 2018. № 11. P. 50–51.*

6. ***Zeng H.*** *Discussion on Network Security Model and Zero-trust Practice // Computer Products and Circulation. 2020. № 7. P. 48.*

7. ***Airport*** *Network Security Protection Scheme Based on Zero Trust Security Architecture / X. Zhong, W. Guo, Y. Ma, M. Wang // Journal of Civil Aviation. 2019. № 3(03). P. 114–116+107.*

O. Prydybailo, R. Prydybailo, V. Yaskevich, Yu. Yaskevich

ZERO TRUST ARCHITECTURE LOGICAL COMPONENTS AND IMPLEMENTATION APPROACHES

Zero Trust Architecture (ZTA) is a contemporary cybersecurity approach that challenges the traditional perimeter-based security model. In the zero-trust model, organizations do not automatically trust any user or device, regardless of whether they are inside or outside the corporate network. Instead, it assumes that threats can come from both internal and external sources, and it verifies every user and device attempting to access resources.

Here are the key principles of this software development trend:

• Identity verification: individuals need to authenticate their identity before gaining access to resources. This often includes multi-factor authentication and reliable verification methods.

• Least privilege access: users are granted the minimum access required to perform their tasks. Access is limited only to essential elements, reducing the potential impact of a security breach.

• Micro-segmentation: involves segmenting the network at a granular level, allowing isolation and protection of individual resources.

• Data encryption: encryption is applied both during transmission and at rest to safeguard data from unauthorized access.

• No implicit trust: applying the principle of "never trust, always verify," meaning verification is necessary at every stage of access.

The article discusses modern challenges and approaches to cybersecurity amidst the rapid development of cloud technologies. Specifically, it analyzes the shift in container usage in software deployment and its impact on the cybersecurity model. Security approaches based on the concept of Zero Trust Architecture (ZTA) are highlighted in the context of new demands and opportunities.

The article elaborates on key logical components of ZTA, such as policy mechanism and policy administrator, pointing out their interaction in creating a secure environment. It also provides an overview of data sources used for creating access policy rules and their consideration in ZTA mechanisms. Additionally, approaches to implementing ZTA for operational workflows in corporate environments are proposed: enhanced identity management, logical micro-segmentation, and network-based segmentation. Each of these approaches has its advantages and is considered based on the needs of individual organizations.

Keywords: architecture; cybersecurity; enterprise; network security; zero trust; zero trust architecture; policy; policy mechanisms.