УДК 004.056.53:65.012.8

DOI: 10.31673/2412-9070.2022.051620

О. Б. ПРИДИБАЙЛО, ст. викладач, здобувач;
І. М. СРІБНА, доктор техн. наук, доцент;
Р. В. ПРИДИБАЙЛО, магістр,
Державний університет телекомунікацій, Київ

АРХІТЕКТУРА НУЛЬОВОЇ ДОВІРИ: ОСНОВНІ ПРИНЦИПИ ОРГАНІЗАЦІЇ

Нульова довіра — це термін для розвивного набору парадигм кібербезпеки, які зміщують захист від статичних мережних периметрів до зосередження на користувачах, активах і ресурсах. Архітектура нульової довіри використовує принципи нульової довіри для планування промислової та корпоративної інфраструктур та робочих процесів. Нульова довіра передбачає відсутність прихованої довіри до активів або облікових записів користувачів виключно на основі їхнього фізичного чи мережного розташування (тобто локальні мережі чи інтернет) або на основі права власності на активи (корпоративні чи особисті). Автентифікація та авторизація (як суб'єкта, так і пристрою) є окремими функціями, які виконуються перед установленням сеансу корпоративного ресурсу. Нульова довіра є відповіддю на тенденції корпоративної мережі, до яких належать віддалені користувачі, застосування власного пристрою і хмарних активів, розташованих за межами корпоративної мережі. Нульова довіра зосереджена на захисті ресурсів (активів, служб, робочих процесів, мережних облікових записів тощо), а не на сегментах мережі, оскільки мережне розташування більше не вважається основним компонентом безпеки ресурсу.

У статті запропоновано абстрактне визначення архітектури нульової довіри і надано загальні моделі розгортання та випадки використання, коли нульова довіра може покращити загальну безпеку інформаційних технологій підприємства. Також описано нульову довіру для архітекторів корпоративної безпеки, яка призначена допомогти цивільним некласифікованим системам зрозуміти її і надати дорожню карту для міграції та розгортання концепцій безпеки нульової довіри в корпоративному середовищі. Починаючи з чіткого розуміння бізнесу та даних організації, можна досягти сильного підходу до нульової довіри для архітекторів корпоративної безпеки.

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

Вступ

Типова інфраструктура підприємства стає дедалі складнішою. Одна установа може керувати кількома внутрішніми мережами, віддаленими офісами з власною локальною інфраструктурою, віддаленими і/або мобільними застосунками та хмарними сервісами. Ця складність випереджає застарілі методи мережної безпеки на основі периметра, оскільки для підприємства не існує єдиного легко ідентифікованого периметра. А отже, мережна безпека на основі периметра також виявилася недостатньою [1].

Таке складне підприємство зумовило розроблення нової моделі кібербезпеки, відомої як ***«нульова довіра»*** **(НД).** Підхід НД здебільшого зосереджено на захисті даних і послуг, але може і розширитись, щоб охопити всі активи підприємства (пристрої, компоненти інфраструктури, програми, віртуальні та хмарні компоненти) і суб'єктів (кінцеві користувачі, програми та інші неживі об'єкти, які запитують інформацію з ресурсів). Моделі безпеки з НД припускають, що в середовищі присутній «зловмисник» і що корпоративне середовище нічим не відрізняється (або не є більш надійним) від будь-якого середовища, яке не належить підприємству. Згідно з цією новою парадигмою підприємство не має припускати прихованої довіри та постійно аналізувати й оцінювати ризики для своїх активів і бізнес-функцій, а потім уводити засоби захисту для пом'якшення цих ризиків. У разі НД ці засоби захисту зазвичай передбачають мінімізацію доступу до ресурсів (зокрема даних та обчислювальних ресурсів та програм/сервісів) лише для тих суб'єктів і активів, визначених як такі, що потребують доступу, а також постійну автентифікацію та авторизацію ідентифікаційних даних і безпеки положення кожного запиту на доступ [2].

Архітектура нульової довіри **(АНД)** — це корпоративна архітектура кібербезпеки, яка базується на принципах нульової довіри та призначена для запобігання витоку даних і обмеження внутрішнього бокового руху.

Відомо, що нульова довіра — це не єдина архітектура, а набір керівних принципів для робочого процесу, проєктування системи та операцій, які можна використовувати для поліпшення стану безпеки будь-якої класифікації чи рівня чутливості. А отже, перехід на АНД — це шлях, що визначає, як організація оцінює ризик у своїй місії, і його не можна подолати просто повною заміною технології. А втім, сьогодні багато організацій уже мають елементи АНД у своїй корпоративній інфраструктурі. Організації повинні прагнути поступово впроваджувати принципи НД, змінювати процеси та технологічні вирішення, які захищають їхні активи даних і бізнес-функції залежно від сценарію використання. Більшість корпоративних інфраструктур спочатку працюватимуть у гібридному режимі нульової довіри/периметра, продовжуючи інвестувати в ініціативи з модернізації ІТ та поліпшувати бізнес-процеси організації.

Щоб ефективність НД була дієвою, організаціям потрібно запроваджувати комплексні методи інформаційної безпеки та стійкості. У поєднанні

з сучасними політиками та вказівками щодо кібербезпеки, керування ідентифікацією та доступом, неперервним моніторингом і найкращими практиками АНД може захистити від типових загроз і вдосконалити стан безпеки організації за допомогою підходу до керування ризиками.

Основна частина

Концепція нульової довіри була відома в кібербезпеці ще до появи терміна «нульова довіра». Робота Єрихонського форуму в 2004 році оприлюднила ідею деперіметризації — обмеження неявної довіри на основі розташування мережі та обмеження покладатися на єдиний статичний захист у великому сегменті мережі. Концепції деперіметризації еволюціонували та вдосконалилися в ширшій концепції нульової довіри, яку пізніше запровадив Джон Кіндерваг під час роботи у Forrester. Потім термін «нульова довіра» став використовуватися для опису різноманітних вирішень кібербезпеки, які віддалили безпеку від неявної довіри, заснованої на мережі. І приватна промисловість, і вища освіта також пройшли цю еволюцію від безпеки на основі периметра до стратегії безпеки, що ґрунтується на принципах нульової довіри.

Коли розпочалося впровадження цих програм, їх було обмежено технічними можливостями інформаційних систем. Політики безпеки були здебільшого статичними та застосовувалися у великих «задушливих точках», які підприємство могло контролювати, аби здобути найбільший ефект за власні зусилля. Із розвитком технології стає можливим неперервний аналіз і оцінювання запитів на доступ динамічним і детальним способом на основі «потреби доступу», щоб пом'якшити вплив даних через скомпрометовані облікові записи, зловмисників, які контролюють мережу, та інші загрози.

Нульова довіра — це парадигма кібербезпеки, зосереджена на захисті ресурсів і передумові, що довіра ніколи не надається неявно, а її потрібно постійно оцінювати. Архітектура нульової довіри — це наскрізний підхід до безпеки корпоративних ресурсів і даних, який охоплює ідентифікацію (особистих і неособових об'єктів), облікові дані, керування доступом, операції, кінцеві точки, хостингові середовища і сполучну інфраструктуру. Початкова увага має бути спрямована на обмеження ресурсів тими, хто потребує доступу та надання лише мінімальних привілеїв (наприклад, читання, запис, видалення), необхідних для виконання місії. Традиційно агенції (і корпоративні мережі загалом) зосереджуються на захисті периметра, а автентифікованим суб'єктам надається авторизований доступ до великої кількості ресурсів у внутрішній мережі. У результаті несанкціоноване переміщення в навколишньому середовищі стало однією з найбільших проблем для федеральних відомств.

Довірені підімкнення до інтернету (ДПІ) і брандмауери периметра агентства забезпечують надійні інтернет-шлюзи. Це допомагає блокувати зловмисників з інтернету, але ДПІ і брандмауери периметра менш корисні для виявлення та блокування атак зсередини мережі та не можуть захистити об'єкти за межами периметра підприємства (наприклад, віддалених працівників, хмарних служб, периферійних пристроїв тощо). Оперативне визначення НД та АНД можна сформулювати так: «Нульова довіра (НД) надає набір концепцій та ідей, призначених для мінімізації невизначеності під час виконання точних рішень щодо доступу з найменшими привілеями для кожного запиту в інформаційних системах і службах. Архітектура нульової довіри (АНД) — це план кібербезпеки підприємства, який використовує концепції нульової довіри та охоплює зв'язки компонентів, планування робочого процесу та політики доступу».

Отже, підприємство з нульовою довірою — це мережна інфраструктура (фізична та віртуальна) і операційні політики, які діють для підприємства як продукт плану архітектури з нульовою довірою.

Спочатку підприємство вирішує прийняти нульову довіру як свою основну стратегію та створити архітектуру нульової довіри як план, розроблений з огляду на принципи НД. Потім цей план розгортається для створення середовища НД для використання на підприємстві.

Наведене визначення зосереджено на суті проблеми, яка полягає в тому, щоб запобігти несанкціонованому доступу до даних і послуг у поєднанні з максимально детальним контролем доступу. Тобто уповноважені та схвалені суб'єкти (комбінація користувача, програми (або служби) і пристрою) можуть отримати доступ до даних за винятком усіх інших суб'єктів (тобто зловмисників). Щоб зменшити невизначеності (оскільки їх неможливо усунути), основну увагу приділяють автентифікації, авторизації та звуженню неявних зон довіри, зберігаючи при цьому доступність і мінімізуючи тимчасові затримки в механізмах автентифікації. Правила доступу створено якомога детальніше, аби забезпечити найменші привілеї, потрібні для виконання дії в запиті.

В абстрактній моделі доступу, зображеній на рис. 1, суб'єкту потрібен доступ до корпоративного ресурсу. Доступ надається через точку ухвалення рішень (ТУР) і відповідну точку застосування політики (ТЗП) [3].

Система має переконатися, що тема є автентичною, а запит дійсним. ТУР/ТЗП ухвалює належне рішення, щоб дозволити суб'єкту отримати доступ

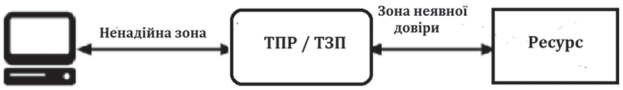

Рис. 1. Доступ із нульовою довірою

до ресурсу. Отже, нульова довіра стосується двох основних сфер: автентифікації та авторизації. Який рівень впевненості щодо особи суб'єкта для цього унікального запиту? Чи дозволений доступ до ресурсу з огляду на рівень впевненості в особистості суб'єкта? Чи пристрій, який використовується для запиту, має належну безпеку? Чи є інші фактори, які слід брати до уваги та які змінюють рівень вірогідності (наприклад, час, місцезнаходження суб'єкта, поза безпеки суб'єкта)? Загалом, підприємству необхідно розробити та підтримувати динамічну політику доступу до ресурсів, що базується на оцінюванні ризику, і налаштувати систему, яка гарантуватиме правильне та послідовне застосування цих політик для окремих запитів на доступ до ресурсів. Це означає, що підприємство не повинно покладатися на неявну надійність, де, якщо суб'єкт відповідає базовому рівню автентифікації (наприклад, вхід в актив), усі наступні запити ресурсів вважаються однаково дійсними.

«Зона неявної довіри» являє собою сферу, де всі об'єкти є довіреними принаймні до рівня останнього шлюзу ТУР/ТЗП. Наприклад, розглянемо модель перевірки пасажирів в аеропорту. Усі пасажири проходять через контрольно-пропускний пункт аеропорту (ТУР/ТЗП), щоб отримати доступ до виходу на посадку. Пасажири, співробітники аеропорту, екіпаж літака тощо перебувають у зоні терміналу, і всі особи вважаються довіреними. У цій моделі неявною зоною довіри є зона посадки.

ТУР/ТЗП застосовує набір елементів керування, щоб увесь трафік поза ТЗП мав загальний рівень довіри. ТУР/ТЗП не може застосовувати додаткові політики за межами свого розташування в потоці трафіку. Щоб дозволити ТУР/ТЗП бути максимально конкретним, неявна зона довіри має бути якомога меншою.

Нульова довіра забезпечує набір принципів і концепцій щодо наближення ТУР/ТЗП до ресурсу. Ідея полягає в тому, щоб чітко автентифікувати та авторизувати всі суб'єкти, активи та робочі процеси, які становлять підприємство.

У багатьох визначеннях і обговореннях НД наголошується на концепції видалення захисту периметра великої зони (наприклад, міжмережних екранів підприємства) як чинника. Однак більшість цих формувань продовжують певним чином визначати себе відносно периметрів (наприклад, мікросегментації або мікроперіметрів) як частину функціональних можливостей АНД.

Архітектуру нульової довіри розроблено та розгорнуто з дотриманням наведених далі основних принципів.

1. Усі джерела даних і обчислювальні послуги вважаються ресурсами. Мережа може мати у своєму складі кілька класів пристроїв. Їй також можуть належати невеликі пристрої, які надсилають дані до агрегаторів/сховищ, програмного забезпечення як послуги (SaaS), систем надсилання інструкцій приводам та інші функції. Крім того, підприємство може вирішувати чи класифікувати особисті пристрої як ресурси, якщо вони можуть отримувати доступ до корпоративних ресурсів.

2. Весь зв'язок захищено незалежно від розташування мережі. Розташування в мережі само собою не означає довіри. Запити на доступ від активів, розміщених у корпоративній мережній інфраструктурі (наприклад, усередині периметра застарілої мережі), мають відповідати такому самому захисту, як запити на доступ та зв'язок із будь-якої іншої мережі, що не належить підприємству. Інакше кажучи, довіра не повинна надаватися автоматично, лише ґрунтуючись на тому, що пристрій перебуває в мережній інфраструктурі підприємства. Усі комунікації мають здійснюватися в найбезпечніший доступний спосіб, підтримуючи захист конфіденційності, цілісності та забезпечення автентифікації джерела.

3. Доступ до окремих ресурсів підприємства надається на основі кожного сеансу. Довіра до запитувача оцінюється перед наданням доступу. Доступ також має бути надано з найменшими привілеями, потрібними для виконання завдання. Це може означати лише «колись нещодавно» для цієї конкретної транзакції і може не відбуватися безпосередньо перед ініціюванням сеансу або виконанням транзакції з ресурсом. Однак автентифікація та авторизація для одного ресурсу не нададуть автоматично доступ до іншого ресурсу.

4. Доступ до ресурсів визначається динамічною політикою, включно з спостережуваним станом ідентичності клієнта, програмами/послугами та активами, що запитує, а також іншими поведінковими та екологічними атрибутами. Організація захищає ресурси за допомогою визначення того, які ресурси вона має, хто є її членами (або здатність автентифікувати користувачів з об'єднаної спільноти) і який доступ до ресурсів потрібен цим членам. Для НД ідентифікатор клієнта може містити обліковий запис користувача (або ідентифікатор служби) і будь-який пов'язаний обліковий запис атрибутів, призначених підприємством цьому обліковому запису, або артефакти для автентифікації автоматизованих завдань. Стан активу запиту може мати такі характеристики пристрою, як версії встановленого програмного забезпечення, розташування в мережі, час/дата запиту, раніше спостережувану поведінку та встановлені облікові дані. До поведінкових атрибутів належать (але цим не обмежуються) автоматизована аналітика

предметів, аналітика пристроїв і виміряні відхилення від спостережуваних моделей використання. Політика — це набір правил доступу на основі атрибутів, які організація призначає суб'єктові, активу даних або програмі. Атрибути середовища можуть охоплювати такі фактори, як місце перебування запитувача в мережі, час, повідомлення про активні атаки тощо. Ці правила та атрибути базуються на потребах бізнес-процесу та прийнятному рівні ризику. Правила доступу до ресурсів і дозволів на дії можуть відрізнятися залежно від чутливості ресурсу/даних. Найменше принципи привілеїв застосовуються для обмеження як видимості, так і доступності.

5. Підприємство відстежує та оцінює цілісність і захист усіх належних і пов'язаних активів. Жоден актив не є надійним. Підприємство оцінює стан безпеки активу під час оцінювання запиту ресурсу. Підприємство, яке впроваджує АНД, має встановити неперервну діагностику та пом'якшення або подібну систему для моніторингу стану пристроїв і застосунків і застосовувати латки/виправлення за потреби. Активи, які виявлено як підривні та мають відомі вразливості і/або якими не керує підприємство, можуть розглядатися інакше (включно з відмовою в усіх під'єднаннях до ресурсів підприємства), ніж пристрої, що належать або пов'язані з підприємством, які вважаються найбільш безпечними. Це також може стосуватися пов'язаних пристроїв (наприклад, особистих пристроїв), яким дозволятиметься доступ до деяких ресурсів, але не до всіх. Водночас це потребує ретельного моніторингу та наявності системи звітності для надання актуальних даних про поточний стан ресурсів підприємства.

6. Уся автентифікація та авторизація ресурсів є динамічними та їх суворо дотримуються доти, доки не буде дозволено доступ. Це неперервний цикл отримання доступу, сканування та оцінювання загроз, адаптації та постійного переоцінювання довіри до поточного спілкування. Очікується, що підприємство, яке впроваджує АНД, матиме системи керування ідентифікацією, обліковими даними та доступом, а також системи керування активами. Це охоплює використання багатофакторної автентифікації (БФА) для доступу до деяких або всіх ресурсів підприємства. Відбувається постійний моніторинг із можливою повторною автентифікацією та повторною авторизацією в усіх транзакціях користувача згідно з визначеною та забезпечуваною політикою (наприклад, на основі часу, запит на новий ресурс, модифікація ресурсу, виявлення аномальної активності суб'єкта), яка прагне досягти балансу безпеки, доступності, зручності використання та економічності.

7. Підприємство збирає якомога більше інформації щодо поточного стану активів, мережної інфраструктури та комунікацій і використовує її для покращення умов безпеки. Підприємство також має збирати дані про запити на доступ, обробляти ці дані та використовувати будь-яку здобуту інформацію для поліпшення, створення та виконання політики. Ці дані також можна застосовувати для надання контексту для запитів на доступ від суб'єктів.

Розглянуті принципи намагаються бути технологічно агностичними. Наприклад, «ідентифікація користувача (ID)» може охоплювати кілька факторів, зокрема ім'я користувача/пароль, сертифікати та одноразовий пароль [4].

Такі принципи застосовуються до роботи, що виконується всередині організації або у співпраці з однією чи кількома партнерськими організаціями, а не до анонімних публічних або орієнтованих на споживачів бізнес-процесів. Організація не може нав'язувати внутрішню політику зовнішнім учасникам (наприклад, клієнтам або звичайним користувачам інтернету), проте здатна впроваджувати деякі політики на основі НД для некорпоративних користувачів, які мають особливі відносини з організацією (наприклад, зареєстровані клієнти, утриманці працівників тощо).

Є кілька основних припущень щодо підімкнення до мережі для будь-якої організації, яка використовує АНД під час планування та розгортання мережі. Деякі з цих припущень застосовуються до корпоративної мережної інфраструктури, а деякі — до корпоративних ресурсів, що працюють на некорпоративній мережній інфраструктурі (наприклад, загальнодоступні Wi-Fi або публічні хмарні постачальники). Ці припущення використовуються для спрямування формування АНД. Мережа на підприємстві, що впроваджує АНД, має бути розроблена з огляду на принципи АНД, викладені раніше, і з наведеними далі припущеннями.

1. Уся корпоративна приватна мережа не вважається неявною зоною довіри. Активи завжди повинні діяти так, ніби зловмисник присутній у корпоративній мережі, а зв'язок має здійснюватися найбезпечнішим доступним способом (див. принцип 2 раніше). Це передбачає такі дії, як автентифікація всіх з'єднань і шифрування всього трафіку.

2. Пристрої в мережі можуть не належати підприємству або налаштовуватися ним. Відвідувачі і/або контрактні послуги можуть мати некорпоративні активи, яким для виконання своєї ролі потрібен доступ до мережі. Це передбачає політику використання власного пристрою, дає змогу суб'єктам підприємства послуговуватися некорпоративними пристроями для доступу до ресурсів підприємства.

3. Жодному ресурсу не можна довіряти. Кожен актив має пройти оцінювання стану безпеки за допомогою ТЗП, перш ніж буде надано запит до корпоративного ресурсу (подібно до принципу 6 для

активів і суб'єктів). Це оцінювання має бути сталим доти, доки сесія триває. Корпоративні пристрої можуть мати артефакти, які уможливлюють автентифікацію та забезпечують вищий рівень вірогідності, ніж той самий запит, що надходить від некорпоративних пристроїв. Самих облікових даних суб'єкта недостатньо для автентифікації пристрою на ресурс підприємства.

4. Не всі ресурси підприємства розміщено в інфраструктурі підприємства. Ресурси мають у своєму складі віддалені суб'єкти підприємства, а також хмарні сервіси. Активам, які належать або керуються підприємством, може знадобитися використання локальної (тобто некорпоративної) мережі для базового підімкнення та мережних послуг (наприклад, вирішення DNS).

5. Віддалені суб'єкти та активи підприємства не можуть повністю довіряти своєму під'єднанню до локальної мережі. Віддалені суб'єкти мають вважати, що локальна (тобто некорпоративна) мережа є ворожою. Активи повинні припускати, що весь трафік відстежується та потенційно змінюється. Усі запити на підімкнення мають бути автентифіковані та авторизовані, і весь зв'язок має здійснюватися максимально безпечним способом (тобто забезпечувати конфіденційність, захист цілісності та автентифікацію джерела).

6. Активи та робочі процеси, що переміщуються між корпоративною та некорпоративною інфраструктурами, повинні мати узгоджену політику та положення безпеки. Активи та робочі навантаження мають зберігати свою безпеку під час переміщення до корпоративної інфраструктури або з неї.

Це стосується пристроїв, які переміщуються з корпоративних мереж у некорпоративні мережі (тобто віддалених користувачів). Це також охоплює робочі навантаження, що переміщуються з локальних центрів оброблення даних до некорпоративних хмарних екземплярів [5].

Висновки

Концепція нульової довіри є широкою, потенційно застосовною до великої кількості варіантів використання та сценаріїв. За приклад може слугувати підприємство з кількома офісами та віддаленими працівниками: географічно розподілені організації, не пов'язані безпосередньо з фізичною мережею. У цьому разі маємо суворо дотримуватися принципу найменших привілеїв. Через неоднорідність у застосованих з'єднаннях та пристроях будь-які облікові дані, надані співробітникам, потенційно можуть бути скомпрометовані та використані для зловмисних дій. Ця концепція поширюється також на локальних відвідувачів та найманих працівників. Застосунок із нульовою довірою може обмежити їх доступ лише до зовнішньої мережі та за замовчуванням заборонити будь-який зв'язок із корпоративними ресурсами. Також ця архітектура дуже важлива для мультихмарних підприємств, в яких джерело даних насамперед із міркувань надмірності та стійкості до відмови розміщене між різними хмарними провайдерами.

Список використаної літератури

1. ***Liu Q.*** *Data center security protection in the industry based on zero-trust architecture // Security & Informatization. 2018. 12. P. 107–109.*

2. ***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.*

3. ***Zuo Y.*** *Zero-trust architecture: a new paradigm for network security // Financial Computerizing. 2018. 11. P. 50–51.*

4. ***Zeng H.*** *Discussion on Network Security Model and Zero-trust Practice // Computer Products and Circulation. 2020. 7. P. 48.*

5. ***Zhong X., Guo W., Ma Y., Wang M.*** *Airport Network Security Protection Scheme Based on Zero Trust Security Architecture // Journal of Civil Aviation, 2019. 3(03). P. 114–116+107.*

O. B. Prydybailo, I. M. Sribna, R. B. Prydybailo

ZERO TRUST ARCHITECTURE: THE BASICS ORGANIZATION PRINCIPLES

Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established. Zero trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud-based assets that are not located within an enterpriseowned network boundary. Zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource. This document contains an abstract definition of zero trust architecture (ZTA) and gives general deployment models and use cases where zero trust could improve an enterprise's overall information technology security posture.

This article describes zero trust for enterprise security architects. It is designed to help understand zero trust for civilian unclassified systems and provide a roadmap for the migration and deployment of zero trust security concepts in an enterprise environment. Starting with a clear understanding of the organization's business and data can lead to a strong zero-trust approach for enterprise security architects.

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