Engineer

Нульова довіра

модель, що не надає довіри лише за розташуванням у мережі

Що це таке

Нульова довіра — це модель безпеки, у якій ніщо не отримує довіри лише через те, де воно розташоване в мережі. NIST SP 800-207, федеральна публікація США, що описала модель у 2020 році, визначає її як парадигму, зосереджену на захисті ресурсів, з вихідною тезою, що довіра ніколи не надається неявно, а має оцінюватися постійно. Перебування в офісній мережі, підключення через VPN чи розміщення в тому самому центрі обробки даних самі собою запиту нічого не дають. Кожен запит до ресурсу вирішується окремо: хто питає, з якого пристрою, про що і за яких умов. В українських текстах часто вживають і англійську назву zero trust, а план, що втілює модель на практиці, називають архітектурою нульової довіри, скорочено ZTA.

NIST чітко називає учасників. Суб'єкт — це той або те, що надсилає запит: людина, сервіс або пристрій. Ресурс — усе, що варто захищати, і публікація зараховує до ресурсів поряд із даними принтери й обчислювальні потужності. Між ними стоять три логічні компоненти. Рушій політик (policy engine) вирішує, чи задовольнити запит, і записує рішення в журнал. Адміністратор політик (policy administrator) виконує це рішення: відкриває або закриває шлях між суб'єктом і ресурсом і видає облікові дані чи токени саме для цього сеансу. Точка застосування політик (policy enforcement point) стоїть на самому шляху: пропускає сеанс, стежить за ним і обриває його, коли отримує таку вказівку.

Публікація пояснює цей зсув на прикладі аеропорту. Пасажири проходять один пункт контролю, а за ним мандрівники, екіпажі та персонал аеропорту вільно ходять терміналом, і всім їм довіряють. Термінал — це те, що NIST називає зоною неявної довіри: простір, де кожному довіряють настільки,

наскільки дозволив останній пройдений пункт контролю. Пласка офісна мережа влаштована так само. Нульова довіра робить цю зону якомога меншою, переносячи рішення та його застосування ближче до ресурсу.

Застосуйте поняття до рішення

Застосуйте «Що таке нульова довіра?» до конкретного рішення. Ми можемо пов'язати поняття із системою, яку ви створюєте або купуєте. Облікові записи, паролі й права налаштовані так, щоб доступ відповідав роботі, а звільнені втрачали його того ж дня.

Переглянути наші послуги Зв'язатися з нами →

Перевірте припущення за терміном

Використайте пояснення та пов'язані роботи, щоб сформулювати запитання для проєкту. Ми можемо перевірити припущення разом до вибору інструмента. Написала 1 000 правил RBAC для Linux-серверів — 1,000 правил доступу написано, щоб усунути вразливість

Написала 1 000 правил RBAC для Linux-серверів Зв'язатися з нами →

Чому це важливо

Стариша модель проводить одну межу довкола організації й довіряє всьому, що всередині. Заперечення NIST просте: щойно зловмисник прорве периметр, він безперешкодно пересувається мережею від системи до системи, і саме такі несанкціоновані бічні переміщення були одним із найбільших викликів для відомств, для яких писали публікацію. До того ж межа більше не відповідає тому, як люди працюють. Співробітники входять із домашніх і готельних мереж, особисті пристрої допускають до частини систем, а значна частина того, з чим люди працюють, розміщена в чужій хмарі. Звідси й припущення NIST: приватна мережа не є зоною неявної довіри, зловмисник може вже бути в ній, а віддалені працівники мають вважати ворожою локальну мережу, до якої підключаються.

Команда виграє на стримуванні. За третьою із семи засад NIST доступ надається на один сеанс із найменшими привілеями, яких потребує завдання, а автентифікація до одного ресурсу не дає нічого щодо іншого. Викрадений пароль чи скомпрометований ноутбук тоді сягає лише того, до чого цей обліковий запис і пристрій мають право доступу в цю мить і через одну точку застосування, а не всієї внутрішньої мережі. Рішення ще й залишають слід. Рушій політик записує кожен дозвіл і кожну відмову, тож на питання, хто міг дістатися системи і чому, відповідають журнали, а не пам’ять.

Як це виглядає на практиці

Візьмімо систему закупівель. Саме такий застосунок NIST радить для першої міграції, бо ним користується визначена група працівників, на відміну від електронної пошти, від якої залежить уся організація. Закупівельник відкриває систему з корпоративного ноутбука. Запит надходить до точки застосування перед нею, а та звертається до рушія політик. Алгоритм довіри рушія зважує вхідні дані, які перелічує NIST: сам запит, зокрема версію операційної системи пристрою та рівень оновлень; базу даних суб'єктів; базу даних активів; власні вимоги ресурсу, що можуть визначати рівень гарантії автентифікації або відхиляти адреси з-за кордону; і відомості про загрози. Ілюстративний запис рішення, з назвами полів, які ми вигадали самі, а не взяли з якогось продукту, міг би виглядати так:

```
запит      buyer-17 з laptop-0417 -> система закупівель, читання і запис
суб'єкт    команда закупівель; вхід ключем, стійким до фішингу
актив      корпоративний пристрій, ОС оновлена, диск зашифровано
ресурс     потрібні AAL2 або вище, керований пристрій, IP-адреса в країні
загроза    адреси джерела немає в перевірених стрічках загроз
рішення    дозволити читання і запис на цей сеанс; записати як схвалене
```

Дозвіл стосується цього одного сеансу й цієї однієї системи. Коли той самий закупівельник на тому самому ноутбуці відкриває договори з постачальниками у сховищі документів, рушій ухвалює нове рішення про доступ: автентифікація до першого ресурсу не надає автоматичного доступу до другого. Важить і контекст. Один із прикладів NIST — бухгалтер, який зазвичай працює в робочі години, а тут посеред ночі просить доступ до фінансової системи з місця, якого рушій не розпізнає: контекстний алгоритм довіри може здійняти тривогу й вимагати, щоб суб'єкт спершу задовольнив суворіший рівень довіри. Інший приклад — працівник відділу кадрів, який у звичайний день переглядає 20–30 особових справ, а потім запитує понад 100.

Для хмарних сервісів NIST зазначає, що клієнти можуть звертатися до сервісу напряму, а точки застосування політик організації перевіряють політику дорогою, замість того щоб спершу заводити клієнтів у внутрішню мережу через VPN. Кожне з цих рішень залежить від чіткої картини того, хто до чого має діставатися, тому NIST радить ще до початку робіт обстежити активи, суб'єктів, потоки даних і робочі процеси. Саме таку підготовчу роботу описує наш кейс про керування доступом у M365 і SSO: облікові записи й доступ

консолідовано в M365, 1Password, Red Hat SSO та OKTA SSO, запроваджено принцип найменших привілеїв, а онбординг і офбординг стандартизовано, тож доступ надавали й відкликали вчасно та послідовно.

Де виникають проблеми

Нульову довіру купують як продукт. NIST наголошує, що нульова довіра — це набір керівних принципів, а не одна архітектура, і що єдиного набору інструментів чи сервісів для підприємства з нульовою довірою не існує. Новий шлюз віддаленого доступу з потрібною наліпкою на коробці мало що змінює, якщо кожен суб'єкт, якого він пропускає, і далі дістається всієї мережі за ним. Розглядайте перехід так, як це робить NIST: як шлях, а не одномоментну заміну всього, і рухайтеся по одному бізнес-процесу. Оцінюйте кожен продукт за тими засадами, які він має забезпечити, зокрема за тим, чи дозволять його формати даних згодом перейти до іншого постачальника.

Політику пишуть раніше за інвентаризацію. Рушій політик може вирішувати лише на підставі того, що знає про суб'єктів, активи й процеси. Там, де ці знання неповні, попереджає NIST, звичайний наслідок — бізнес-процес, що зупиняється, бо рушій відхиляє запити через брак відомостей, а тіньові IT, тобто системи, розгорнуті поза контролем IT-відділу, лише погіршують справу. Спершу обстежте й опишіть активи, суб'єктів, потоки даних і робочі процеси, тіньові IT включно, і лише потім пишіть критерії для процесу, який переносите.

Адміністратори зберігають повний доступ. У багатьох застарілих архітектурах безпеки розробники й системні адміністратори можуть дістатися будь-якого ресурсу, і NIST окремо виділяє ці облікові записи для посиленої уваги. Якщо всіх інших перевести на рішення для кожного сеансу, а адміністраторським обліковим записам лишити їхній постійний доступ, найцінніші облікові дані стануть найкоротшим шляхом усередину. Тож пропускайте й привілейовані облікові записи через той самий рушій, давайте їм той доступ, якого потребує поточне завдання, і за допомогою журналювання та аудиту вивчайте їхні звичні шаблони, щоб відхилення одразу впадали в око.

Рушій політик стає новим периметром. Жоден ресурс не спілкується з іншим без схвалення рушія та адміністратора. Будь-хто з доступом до правил рушія може внести несхвалені зміни або просто помилитися, а зловмисник,

що порушить роботу точок застосування чи адміністратора, здатен зупинити бізнес. Тож журналюйте й перевіряйте кожну зміну конфігурації, розгорніть застосування політик у належно захищеному хмарному середовищі або продублюйте його в кількох місцях, а збереженим даним про мережу та політиці надайте найсуворіший доступ із усіх, лише з окремих адміністраторських облікових записів.

Усе застосовують із першого дня. Мало які набори політик правильні з першої спроби, і NIST очікує етапу налаштування, коли запити, які мали б пройти, відхиляються. Якщо одразу перейти до суворого застосування, кожна прогалина в політиці обернеться працівниками, відрізаними від потрібної їм роботи. Натомість якийсь час запускайте новий робочий процес у режимі, де рішення лише фіксуються у звітах. Задовольняйте більшість запитів, порівнюйте журнали із задуманою політикою й застосовуйте лише базове, наприклад відмову для запитів, що не пройшли MFA або надходять з адрес, відомих як ворожі. Посилюйте політику, коли звичний шаблон стане зрозумілим.

MFA вважають фінішною лінією. MFA знижує ризик від викраденого пароля, але NIST зазначає, що зловмисник із чинними обліковими даними або зловмисний інсайдер усе одно дістанеться всього, до чого має доступ обліковий запис. Тримайте доступ кожного облікового запису вузьким і застосовуйте контекстний алгоритм довіри, що враховує час, місце та обсяг, щоб чинні облікові дані, використані незвично, теж здіймали тривогу.

Що почитати далі

- NIST SP 800-207, Zero Trust Architecture — опублікована в серпні 2020 року: визначення, сім засад, логічні компоненти, загрози та дорожня карта переходу.
- NIST SP 1800-35, Implementing a Zero Trust Architecture — практичний посібник NIST, опублікований у червні 2025 року, з описом 19 прикладів реалізації, створених разом із 24 партнерами.
- NIST SP 800-207A — опублікована у вересні 2023 року: контроль доступу для хмарно-нативних застосунків у кількох хмарах на основі API-шлюзів, проксі-контейнерів sidecar та ідентичностей сервісів замість мережевих адрес.
- NIST SP 800-63B-4 — рівні гарантії автентифікації, на які можуть посилатися вимоги ресурсу; AAL3 з них вимагає стійкості до фішингу.

Словник

Обирайте за фактичними умовами

Опишіть шлях розгортання, експлуатаційні ризики та чергову команду. Ми можемо визначити зміну з перевірками, шляхом відновлення та чіткою відповідальністю.

Дивитися, скільки це коштує Зв'язатися з нами →

Зробіть термінологію практичною

Запитайте, як «Що таке нульова довіра?» стосується вашої організації. Конкретного прикладу з поточної системи достатньо для початку розмови.

Переглянути наші послуги

welcome@engineer.company +45 50 10 61 84 Копенгаген, Данія

Візьміть цю сторінку із собою

Візитівка

Дбайливо зроблено з любов'ю — D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Авторське право © 2025 – дотепер · Engineer ApS · Усі права захищено.

Надруковано з https://engineer.company/uk/glossary/zero-trust/