Полотай Орест Іванович, кандидат технічних наук, доцент

Львівський державний університет безпеки життєдіяльності, м.Львів

https://orcid.org/0000-0003-4593-8601

**ZERO TRUST ARCHITECTURE: НОВИЙ СТАНДАРТ БЕЗПЕКИ КОРПОРАТИВНИХ МЕРЕЖ ПІДПРИЄМСТВА**

У сучасному цифровому світі, де бізнес-процеси дедалі активніше переміщуються в онлайн-середовище, проблема кібербезпеки набуває нового значення. Класичні моделі захисту, побудовані за принципом периметра, більше не здатні ефективно протистояти зростаючій кількості загроз. В умовах, коли співробітники працюють з дому, використовують особисті пристрої, а корпоративні ресурси розміщуються у хмарі, ідея надійного "захищеного кордону" втрачає сенс. Саме в цьому контексті формується новий підхід до безпеки – Zero Trust Architecture (ZTA), який поступово стає новим стандартом для організацій будь-якого масштабу.

Основні концепції моделі нульової довіри – це постійна (не одноразова) автентифікація користувачів і пристроїв, шифрування всіх ресурсів, надання мінімального доступу та обмеження його тривалості, сегментація для мінімізації наслідків порушень безпеки даних [4].

Архітектура Zero Trust базується на простій, але радикальній ідеї: не довіряти нікому і нічому за замовчуванням, незалежно від того, чи знаходиться об'єкт доступу всередині, чи поза межами корпоративної мережі. Усе, що відбувається в системі, має бути ретельно перевірене, контрольоване та логовано. Доступ до будь-якого ресурсу надається лише після підтвердження ідентичності, оцінки контексту, аналізу поведінки користувача і відповідності політикам безпеки.

Архітектура нульової довіри – це стратегія кібербезпеки підприємства, що базується на принципах нульової довіри та включає взаємодію між компонентами системи, організацію робочих процесів і політики контролю доступу» – національний інститут стандартів і технологій (NIST) [1].

Універсальний алгоритм впровадження Zero Trust Architecture на стандартному підприємстві показаний в таблиці 1.

Таблиця 1

Алгоритм запровадження архітектури нульової довіри на підприємстві

|  |  |
| --- | --- |
| Дія | Характеристика |
| Ініціалізація стратегії Zero Trust | На цьому етапі підприємство формулює чітке бачення Zero Trust як не просто технічної моделі, а загально-організаційної стратегії. Визначається відповідальна команда, готуються документи, презентації для керівництва, затверджується бюджет і часові рамки проєкту. |
| Інвентаризація активів та класифікація ресурсів | Проводиться повна інвентаризація:* користувачів і ролей,
* пристроїв (комп’ютери, телефони, IoT),
* додатків і сервісів,
* мережевих вузлів,
* даних (класифікація за критичністю: публічні, конфіденційні, секретні).

Цей крок формує базу для подальшої сегментації та політик контролю доступу. |
| Визначення “зони довіри” — сегментація середовища | Мережа ділиться на ізольовані логічні зони або мікросегменти. Наприклад:* зона для фінансових систем,
* зона для розробників,
* зона для гостьових пристроїв.

Кожна зона має чітко обмежений набір дозволених комунікацій. Всі міжзональні з'єднання проходять через контролюючі точки (наприклад, мікрофаєрволи, проксі або внутрішній шлюз). |
| Впровадження механізмів перевірки ідентичності | Будується централізована система ідентифікації та управління доступом (Identity & Access Management – IAM). До цього включається:* єдиний вхід (SSO),
* багатофакторна автентифікація (MFA),
* контекстуальна автентифікація (геолокація, поведінкові патерни),
* політики Least Privilege Access (доступ лише до необхідного).
 |
| Аналіз і оцінка контексту доступу | Доступ до ресурсів надається лише після оцінки:* хто (ідентичність),
* з чого (тип пристрою, стан безпеки),
* звідки (мережа, геолокація),
* коли (час, частота звернення),
* навіщо (тип запиту, ризик дії).

Застосовуються системи умовного доступу (Conditional Access) і правила, які можуть автоматично відмовити у доступі або запустити додаткову перевірку. |
| Впровадження безперервного моніторингу та аналітики [2]. | Усі дії користувачів і пристроїв фіксуються в логах. Важливо інтегрувати SIEM-систему, яка збирає, корелює та аналізує події в режимі реального часу.Також впроваджується система поведінкового аналізу (UEBA) для виявлення аномалій, наприклад, раптових нічних входів, великих завантажень даних, невластивих дій. |
| Автоматизація реакцій на інциденти | Інтегруються SOAR-рішення (Security Orchestration, Automation, and Response), які здатні автоматично реагувати на певні інциденти: наприклад, ізоляція пристрою, примусове завершення сесії, блокування облікового запису. |
| Постійна оптимізація та аудит політик | Zero Trust – це не одноразовий проєкт, а постійний процес. Рекомендується:* проводити регулярні аудити політик доступу,
* переглядати права користувачів щокварталу,
* оновлювати правила доступу відповідно до змін у структурі компанії,
* здійснювати пентести і Red Team вправи [3].
 |

Ця модель підходить як для середніх, так і для великих підприємств, і легко масштабована. Ключ до успіху – інтеграція безпеки на всіх рівнях: мережа, користувач, пристрій, додаток, дані.

**Література**

1. Коробейнікова Т.І., Журавель І.М., Бодак А.О., Бороденко Д.В. Концепція нульової довіри: сучасні методи забезпечення кібербезпеки в корпоративних мережах. Вісник Львівського державного університету безпеки життєдіяльності. 2024. № 30. С. 67-77
2. Полотай О.І., Пузир А.О. Аналіз та впровадження засобів запобігання витоку конфіденційної інформації на підприємствах, на прикладі системи DLP. Вісник Львівського державного університету безпеки життєдіяльності. 2024. № 30. С. 134-144
3. Полотай О.І., Сусяк Р.Я. Особливості проекту підвищення рівня обізнаності працівників підприємств в сфері кібербезпеки. “Світ наукових досліджень” (матеріали Міжнародної мультидисциплінарної наукової інтернет-конференції (м. Тернопіль, Україна, м. Ополе, Польща, 23-24 квітня 2024 р.). Вип. 29. С. 257-259.
4. Принцип дії архітектури нульової довіри. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-zero-trust-architecture